

[2020] PDP Digest

PERSONAL DATA PROTECTION DIGEST



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

PERSONAL DATA PROTECTION DIGEST

Editor

Yeong Zee Kin

Deputy Editors

Chen Su-Anne

Adeline Chung

Teo Xuan Lang



2020

CITATION

This volume may be cited as:
[2020] PDP Digest

DISCLAIMER

Views expressed by the article contributors are not necessarily those of the Personal Data Protection Commission (“PDPC”), the Editors nor the Publisher (Academy Publishing). Whilst every effort has been made to ensure that the information contained in this work is correct, the contributors, PDPC and the Publisher disclaim all liability and responsibility for any error or omission in this publication, and in respect of anything, or the consequences of anything, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication.

COPYRIGHT

© 2020 Personal Data Protection Commission

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.

All rights reserved. No part of this publication may be reproduced, stored in any retrieval system, or transmitted, in any form or by any means, whether electronic or mechanical, including photocopying and recording, without the written permission of the copyright holder. All enquiries seeking such permission should be addressed to:

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) 024/07/2020

FOREWORD

BY THE PERSONAL DATA PROTECTION COMMISSIONER

Over the past few years, Singapore has positioned and developed itself as a regional data hub. To maintain this lead, it is necessary to have forward-thinking policies. This includes an evolving data protection regime that not only responds to but stimulates a dynamic data industry.

The *Personal Data Protection Digest* (“Digest”) is one of the Personal Data Protection Commission’s (“PDPC”) yearly initiatives. It is the only publication globally, by a regulator, that encourages active contribution from the data protection community. The intent is to encourage a deepening in thoughtfulness and development of views by providing a focal point for discourse. This in turn will enable all in the data protection community to benefit from the sharing of knowledge and views. As with the Digest of previous years, this year’s Digest contains articles contributed by data protection practitioners, who share their insights and practical tips with regard to data protection and managing data incidents. These contributions elucidate the underlying principles of Singapore’s data protection laws and policies, from which good organisational practices may be derived. Over the years, we have seen an increasing level of sophistication in the discussions and views put forth in the articles penned by our data protection community. This year is no different. We are heartened by the excellent articles contributed by the authors. These demonstrate the eagerness of our local practitioners to take on global thought leadership in this area.

Several contributors have also helpfully discussed the use of data for business improvement, innovation and legitimate interests, and the proposed introduction of safe harbours to the Personal Data Protection Act (“PDPA”) that could further facilitate these purposes. One major impetus for these safe harbours is the advent of big data. In the current digital economy, access to and analysis of datasets can help organisations tremendously in decision-making, facilitate innovation and boost their competitiveness. It is heartening that even as we have consulted on these new policy initiatives and the draft Personal Data Protection (Amendment) Bill, the discussion has already started. To complement the proposed legislative changes, the PDPC is looking into better addressing the need of organisations for clarity on when and how they may make use of data. This

will involve, amongst other things, clarifying the boundaries between regulated data (*ie*, data falling within the scope of the PDPA) and unregulated data, for instance, personal data that has been anonymised such that reidentification risk is negligible. We also plan to develop simple charts and tables to help data protection officers and practitioners understand the interactions between the different types of exceptions and consent.

Going forward, the PDPC will continue to engage with the industry in navigating new pertinent areas of data protection such as biometrics and data ethics. The PDPC will partner the industry to identify the issues and concerns, and develop practical solutions and best practices. We anticipate that the process will be an iterative one due to the nascence of these areas, and we recognise the need for open exchanges with stakeholders. We believe that the partnership will help us achieve clarity and certainty in our positions on the issues, so that technology can reach the hands of businesses and consumers in a tangible form more quickly.

We thank the authors of the articles for their contributions to the Digest. I hope that you will find the Digest informative and useful in providing guidance on how businesses can operate effectively in the digital economy in accordance with the PDPA.

Lew Chuen Hong

Commissioner

Singapore

CONTENTS

	Page
<i>Foreword by the Personal Data Protection Commissioner, Lew Chuen Hong</i>	iii
Articles	
<i>Strengthening Accountability and Consumer Trust</i>	
Appointing a Data Protection Officer – In or Out? <i>Philip CHONG and YEOH Lian Chuan</i>	1
Use of Data for Business Improvement – Beyond Rights <i>LEE Soo Chye, TEO Yi Ting Jacqueline and Vera KOH Li Juen</i>	12
Being Accountable in Transforming Your Business for Data Innovation – Learning Points from the Personal Data Protection Commission’s Enforcement Decisions in 2019 <i>Steve TAN and Justin LEE</i>	23
<i>Promoting Innovation and Supporting the Growth of Singapore’s Digital Economy</i>	
Data Portability: Striking the Right Balance between the Individual and “Data Controller” <i>Charmian AW, Cynthia O’DONOGHUE and Sarah BRUNO</i>	34
Data Localisation: The Way Forward or Backward for Data Innovation? <i>Lanx GOH and Joshua KOW</i>	63
The Expanding Role of the Retention Limitation Obligation in the Modern Day <i>Jansen AW and Kenneth TAN</i>	72
<i>Managing Data Incidents</i>	
Preventing and Managing Data Incidents: Lessons from the Personal Data Protection Commission’s Enforcement Decisions <i>LIM Chong Kin and Janice LEE</i>	87
Implementing Data Breach Programmes: Understanding Nuances in Practice and the Personal Data Protection Act <i>LIM Sui Yin, Jeffrey</i>	103
Lessons on Managing Breaches in Singapore from One Year of the General Data Protection Regulation <i>Bryan TAN</i>	120

	Page
<i>Rights and Treatment of Individuals under the Personal Data Protection Act 2012</i>	
The Personal and Domestic Exclusion <i>Benjamin WONG YongQuan</i>	130
First Do No Harm: Protecting Patient Data in the Modern Age <i>Benjamin GAW and Charis SEOW</i>	140
Civil Proceedings under the Personal Data Protection Act 2012 <i>Alexander YAP Wei-Ming, TAY Yong Seng, ANG Ann Liang and Brenda SOH</i>	154
Grounds of Decisions	
<i>Re Tutor City</i> [2020] PDP Digest 170; [2019] SGPDPC 5	170
<i>Re PAP Community Foundation</i> [2020] PDP Digest 180; [2019] SGPDPC 6	180
<i>Re Matthew Chiong Partnership</i> [2020] PDP Digest 185; [2019] SGPDPC 7	185
<i>Re German European School Singapore</i> [2020] PDP Digest 198; [2019] SGPDPC 8	198
<i>Re H3 Leasing</i> [2020] PDP Digest 215; [2019] SGPDPC 9	215
<i>Re Option Gift Pte Ltd</i> [2020] PDP Digest 219; [2019] SGPDPC 10	219
<i>Re Ncode Consultant Pte Ltd</i> [2020] PDP Digest 226; [2019] SGPDPC 11	226
<i>Re Starhub Mobile Pte Ltd and others</i> [2020] PDP Digest 234; [2019] SGPDPC 12	234
<i>Re Skinny's Lounge</i> [2020] PDP Digest 248; [2019] SGPDPC 13	248
<i>Re Grabcar Pte Ltd</i> [2020] PDP Digest 252; [2019] SGPDPC 14	252
<i>Re Grabcar Pte Ltd</i> [2020] PDP Digest 265; [2019] SGPDPC 15	265
<i>Re DS Human Resource Pte Ltd</i> [2020] PDP Digest 274; [2019] SGPDPC 16	274
<i>Re InfoCorp Technologies Pte Ltd</i> [2020] PDP Digest 282; [2019] SGPDPC 17	282

Contents

	Page
<i>Re Cigna Europe Insurance Company SA-NV</i> [2020] PDP Digest 286; [2019] SGPDPDC 18	286
<i>Re Xbot Pte Ltd</i> [2020] PDP Digest 292; [2019] SGPDPDC 19	292
<i>Re AIA Singapore Private Limited</i> [2020] PDP Digest 298; [2019] SGPDPDC 20	298
<i>Re SME Motor Pte Ltd</i> [2020] PDP Digest 306; [2019] SGPDPDC 21	306
<i>Re Spize Concepts Pte Ltd</i> [2020] PDP Digest 311; [2019] SGPDPDC 22	311
<i>Re AgeDesign Pte Ltd</i> [2020] PDP Digest 322; [2019] SGPDPDC 23	322
<i>Re The Central Depository (Pte) Limited and another</i> [2020] PDP Digest 325; [2019] SGPDPDC 24	325
<i>Re Champion Tutor Inc</i> [2020] PDP Digest 342; [2019] SGPDPDC 25	342
<i>Re Genki Sushi Singapore Pte Ltd</i> [2020] PDP Digest 347; [2019] SGPDPDC 26	347
<i>Re Horizon Fast Ferry Pte Ltd</i> [2020] PDP Digest 357; [2019] SGPDPDC 27	357
<i>Re Avant Logistic Service Pte Ltd</i> [2020] PDP Digest 371; [2019] SGPDPDC 28	371
<i>Re Friends Provident International Limited</i> [2020] PDP Digest 377; [2019] SGPDPDC 29	377
<i>Re Executive Link Services Pte Ltd</i> [2020] PDP Digest 381; [2019] SGPDPDC 30	381
<i>Re Learnaholic Pte Ltd</i> [2020] PDP Digest 387; [2019] SGPDPDC 31	387
<i>Re O2 Advertising Pte Ltd</i> [2020] PDP Digest 398; [2019] SGPDPDC 32	398
<i>Re Amicus Solutions Pte Ltd and another</i> [2020] PDP Digest 404; [2019] SGPDPDC 33	404
<i>Re Marshall Cavendish Education Pte Ltd</i> [2020] PDP Digest 425; [2019] SGPDPDC 34	425
<i>Re Advance Home Tutors</i> [2020] PDP Digest 438; [2019] SGPDPDC 35	438
<i>Re Singapore Telecommunications Limited</i> [2020] PDP Digest 448; [2019] SGPDPDC 36	448

Contents

	Page
<i>Re Zero1 Pte Ltd and another</i> [2020] PDP Digest 458; [2019] SGPDPDC 37	458
<i>Re EU Holidays Pte Ltd</i> [2020] PDP Digest 467; [2019] SGPDPDC 38	467
<i>Re Ninja Logistics Pte Ltd</i> [2020] PDP Digest 473; [2019] SGPDPDC 39	473
<i>Re SearchAsia Consulting Pte Ltd</i> [2020] PDP Digest 481; [2019] SGPDPDC 40	481
<i>Re i-vic International Pte Ltd</i> [2020] PDP Digest 485; [2019] SGPDPDC 41	485
<i>Re The Travel Corporation (2011) Pte Ltd</i> [2020] PDP Digest 489; [2019] SGPDPDC 42	489
<i>Re MSIG Insurance (Singapore) Pte Ltd and another</i> [2020] PDP Digest 495; [2019] SGPDPDC 43	495
<i>Re Chizzle Pte Ltd</i> [2020] PDP Digest 506; [2019] SGPDPDC 44	506
<i>Re SAFRA National Service Association</i> [2020] PDP Digest 511; [2019] SGPDPDC 45	511
<i>Re National Healthcare Group Pte Ltd</i> [2020] PDP Digest 517; [2019] SGPDPDC 46	517
<i>Re PeopleSearch Pte Ltd</i> [2020] PDP Digest 525; [2019] SGPDPDC 47	525
<i>Re Society of Tourist Guides (Singapore)</i> [2020] PDP Digest 531; [2019] SGPDPDC 48	531
 Case Summaries	
<i>Re Barnacles Pte Ltd</i>	539
<i>Re Campvision Ltd</i>	541
<i>Re ERGO Insurance Pte Ltd</i>	542
<i>Re Global Outsource Solutions Pte Ltd</i>	544
<i>Re Honestbee Pte Ltd</i>	546
<i>Re iClick Media Pte Ltd</i>	548
<i>Re Saturday Club Pte Ltd</i>	549
<i>Re Tan Tock Seng Hospital Pte Ltd</i>	550

APPOINTING A DATA PROTECTION OFFICER – IN OR OUT?*

Philip CHONG[†]

Global Leader Digital, AI Controls, Algorithm, Deloitte

YEOH Lian Chuan[†]

Managing Director, Sabara Law LLC

1. Accountability and the role of the data protection officer

1 In today's increasingly connected and data-rich world, individuals are naturally and quite rightly more aware and concerned about risks around the unauthorised collection, use and disclosure of personal data.

2 This has led to a recognition that organisations must move from a compliance-based tick-box approach to personal data protection towards a more accountability-based framework.

3 What is accountability? In essence, it is the “undertaking and demonstration of responsibility” for the personal data in the organisation's possession or control. The focus is on the assumption of responsibility by an organisation for the personal data which it possesses or controls.

4 Furthermore, in forward-looking companies, the role of a data protection officer (“DPO”) has increasingly gone beyond a traditional compliance function and includes being a *strategic adviser* on the responsible and innovative use of personal data.

5 To discharge these functions, it is also increasingly expected that the DPO will be a part of, or at least report directly to, the senior leadership team or management committee within an organisation.

* 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.

† The authors wish to thank Sheryl Khoo for her assistance in the preparation of this article.

A. Provisions on accountability and role of the DPO in the Personal Data Protection Act 2012

6 Sections 11 and 12 of the Personal Data Protection Act 2012¹ (“PDPA”) form the basic statutory building blocks of the Accountability Obligation under the PDPA. These sections require that an organisation:

- (a) develop and implement data protection policies² and communicate these to its staff;³
- (b) develop a process to receive and respond to complaints;⁴
- (c) upon request, provide information to the public about its data protection policies and complaints process;⁵ and
- (d) designate “one or more individuals to be responsible for ensuring that the organisation complies with the” PDPA.⁶ Such a person is commonly known as a “data protection officer”, or “DPO”.

7 A DPO may delegate to another individual the responsibility conferred by the designation.⁷ The Personal Data Protection Commission (“PDPC”) has suggested that this need not be a full delegation but may be a partial delegation of certain responsibilities only.⁸

8 The appointment of a DPO does not relieve an organisation of any of its obligations under the PDPA.⁹

1 Act 26 of 2012.

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 12(a). Paragraph 20.9 of the Personal Data Protection Commission’s *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) goes on to note that “organisations should develop both internal and external policies and practices”, and also that the “organisation should also put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices”.

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

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

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

6 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(3).

7 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(4).

8 See para 20.3 of the Personal Data Protection Commission’s *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019).

9 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(6).

9 The PDPC’s *Guide to Developing a Data Protection Management Programme*¹⁰ (“DPM Programme Guide”) elaborates on the role of a DPO as follows:¹¹

- (a) ensuring compliance with the PDPA through data protection policies and processes;
- (b) fostering a personal data protection culture and communicating personal data protection policies to stakeholders;
- (c) handling access and correction requests to personal data;
- (d) managing personal data protection-related queries and complaints;¹²
- (e) alerting management to any risks that might arise with regard to the personal data handled by the organisation; and
- (f) liaising with the PDPC on personal data protection matters, if necessary.

B. Some observations regarding a DPO’s role

10 The authors would venture a few observations about the role of the DPO under the PDPA.

11 First, the DPO must be an *individual*. There is no such thing as a corporate DPO, although it is entirely possible for an organisation to engage a service provider to furnish an employee or other nominee of the provider to serve as a DPO.

12 Second, the words used in s 11(3) of the PDPA to describe the DPO’s functions appear to be very broadly cast. The DPO is described as a person “responsible for ensuring that the organisation complies with” the PDPA – and this might be a concern for third parties seeking to assume the role of a DPO, a point to which the authors will return below. By contrast, for example, in Art 39 of the General Data Protection Regulation¹³ (“GDPR”) of the European Union (“EU”), a DPO’s tasks are defined more specifically, and include:

10 Revised 15 July 2019.

11 Personal Data Protection Commission, *Guide to Developing a Data Protection Management Programme* (revised 15 July 2019) at para 3.2.

12 However, see the comments in the following passages.

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

- (a) to *inform and advise* the data comptroller and processor, and employees who carry out processing, of their obligations;
- (b) to *monitor compliance*, including awareness raising and training;
- (c) to provide advice when requested on data protection impact assessments (“DPIAs”); and
- (d) to co-operate and act as a contact point for the supervisory authority.

13 Third, an organisation may appoint one or more DPOs, and this raises the question of whether it is generally better to appoint multiple DPOs, or a single DPO even if he is supported by others with relevant skills and expertise. The authors favour the view that, in general, it would be better (for accountability reasons) to designate a single DPO,¹⁴ on account of the judgment and subjectivity of many decisions which a DPO would take. However, even in this scenario, it is likely that the DPO will require the support of a team, given the range of diverse skills required.

14 Fourth, with respect to the functions mentioned in paras 9(c) and 9(d) above, reg 3(2)(b) of the Personal Data Protection Regulations 2014¹⁵ specifically provides that data subject access and correction requests should be made to the DPO.

15 However, not all requests by data subjects must go through the DPO. For instance:

- (a) section 20(1)(c) of the PDPA provides that an organisation must, upon an individual’s request, provide the individual with the business contact information of a person who is able to answer the individual’s questions about the collection, use or disclosure of personal data; and
- (b) section 20(4)(b) of the PDPA contains a similar provision in respect of questions by employees regarding the personal data

14 This view is also expressed by the author of the International Association of Privacy Professionals’ *DPO Handbook* (2nd Ed, 2018) ch 2, where it was said that “one person in the DPO team should always be designated to have the final vote on all [data protection] issues and that person should carry the designation of DPO”. *Cf* the position taken in the Personal Data Protection Commission’s *Guide to Developing a Data Protection Management Programme* (revised 15 July 2019) at para 3.2.1.

15 S 362/2014.

collected, used or disclosed in connection with the management or termination of an employment relationship.

16 In the cases described in the previous paragraph, it would be quite understandable if an organisation thought that its front-line customer-facing staff or the human resources department may be better placed to address the query, although it is possible for the contact of the DPO to be given as well (possibly as an alternative).

17 In the case of complaints, the PDPA appears to be silent as to whether the DPO must be designated as the point of contact, but in the authors' view, the DPO would be the natural point of contact. It may also be noted that, in any case, s 11(5) of the PDPA requires an organisation to make available to the public the business contact of at least one DPO (or his delegate) and this would normally be done in the organisation's externally-facing data protection policy.

18 Fifth, it is noteworthy that, in the EU, the GDPR envisages that the DPO is subject to independence requirements¹⁶ and must avoid other roles which create a conflict of interest.¹⁷ A number of roles, such as the human resources and information technology director, chief marketing officer and chief information security officer, may be incompatible with the DPO role. While the PDPC's *Guide to Accountability under the Personal Data Protection Act* does suggest that it is preferable if a DPO were appointed "from senior management, who can effectively direct and oversee data protection initiatives", similar "hard" requirements of independence and non-conflict under the GDPR do not exist under the PDPA. Also, notwithstanding the comment noted above that having senior management assume the DPO role would generally be desirable, it is nonetheless clear

16 Article 38(3) of the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) provides that: "The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."

17 Article 38(6) of the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) provides that: "The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."

that a DPO need not be an officer or employee of the organisation but may be an individual or individuals provided by a third-party service provider. However, in such a situation, para 3.2.1 of the DPM Programme Guide envisages that “the organisation should still ensure that an individual appointed from senior management remains responsible to work with the outsourced DPO”.

19 Sixth, there is no requirement in Singapore that the DPO must be based locally. However, the business contact information of the DPO should be readily accessible from Singapore, operational during Singapore business hours and, in the case of telephone numbers, be Singapore telephone numbers.¹⁸

20 Seventh, the role of a DPO is *not universal* in data protection regimes globally. For example, in China, Hong Kong Special Administrative Region,¹⁹ Malaysia or Japan, there is no requirement to appoint a DPO. Conversely, such requirements exist in South Korea and the Philippines. In the EU, the appointment of a DPO under the GDPR is mandatory only if an organisation’s core activities consist of processing:

- (a) operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale;
- (b) sensitive personal data on a large scale.

21 In Singapore, however, *every* organisation – no matter how large or small – must appoint a DPO (including a sole proprietor). The means that the range of organisations which must appoint a DPO is extremely wide, and may range from a small one-man organisation that processes little personal data to a large corporate which holds large amounts of highly sensitive personal data. It would be little surprise to think that such a varied range of organisations may approach the question of using internal *versus* external resources to satisfy their duty to appoint a DPO differently, and the authors therefore now turn to some of the considerations which an organisation could take into account when making such a determination.

18 See para 20.7 of the Personal Data Protection Commission’s *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019).

19 Although this is recommended by the Privacy Commissioner for Personal Data as a “best practice”.

II. Considerations for appointing an internal *versus* external DPO

22 The skill sets²⁰ relevant to the role of a DPO are diverse and include knowledge within the following domains:

- (a) the laws relating to data protection²¹ and related domains;
- (b) knowledge of technical data protection measures;
- (c) security risk assessment, audit, certification standards and mitigation;
- (d) emerging areas such as data governance, data ethics, artificial intelligence and data sharing; and
- (e) other “soft” skills such as leadership, negotiation, project management, communication, self-drive, ability to relate to others, *etc.*

It may be observed that it is (unsurprisingly) uncommon for one individual to be a master of all the above skill sets.

23 The models of delivery for data protection services by external data protection providers are also varied,²² but may broadly be divided into the following categories:

- (a) general training services;
- (b) the provision of electronic tools and aids and/or specific audit, advisory and consulting services (*eg*, preparation of data inventory and record of processing activities, risk and controls registers, drafting policies and procedures, breach response management support, *etc*) or an on-site resource (perhaps on a *per diem* basis) provided to an organisation whose employee nonetheless remains the DPO; or

20 Also see the nine competencies in the Personal Data Protection Commission’s *DPO Competency Framework and Training Roadmap* <<https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap>> (accessed 1 June 2020), which slices the pie somewhat differently from the way the authors have done in the text.

21 Interestingly, Art 37(5) of the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018) referred specifically to “expert knowledge of data protection law and practice”.

22 A list of data protection service providers may be found at <<https://www.pdpc.gov.sg/help-and-resources/2020/03/list-of-data-protection-service-providers>> (accessed 1 June 2020).

- (c) outsourcing the actual role of the DPO to an individual employee or nominee of the corporate service provider.

24 Other considerations relevant to the appointment of an internal *versus* external DPO would include the following:

- (a) Generally speaking, an internal DPO candidate would be expected to have greater:
 - (i) knowledge and familiarity with the organisation's business;²³
 - (ii) availability of time to devote to the role; and
 - (iii) ability to influence decisions at the level of top management.
- (b) In some organisations, internal resources able to meet the diverse range of skill sets required to ensure compliance with the PDPA and discharge the responsibilities of a DPO may simply not exist. An outsourced DPO service provider would likely be able to bring to bear from its own organisational resources a wide(r) range of the relevant skill sets. An external DPO may also be able to bring to bear experiences derived from his work for other organisations and industry sectors.
- (c) Given the broad definition of the role of a DPO in s 11(3) of the PDPA, the potential legal liability exposure would be a potential concern for a third-party DPO. Hence, it may be expected that, in the outsourcing agreement for the engagement of a DPO, the limitation of liability clause would attract some attention. Conversely, the organisation would have concern if the data protection law envisaged the prospect of substantial fines. It is also of note that the PDPA itself does not envisage that the PDPC could impose directions (including financial penalties) directly on a DPO, so the prospect of liability is generally mediated through the organisation.
- (d) Considerations of cost – on an hour-for-hour basis, an internal resource would generally be cheaper. However, if an

23 Although as noted at para 18 above, the Personal Data Protection Commission has indicated the view that a member of senior management would be expected to work with an external data protection officer.

organisation engaged an internal DPO, the remuneration of the relevant personnel would become a fixed cost.

- (e) Considerations relating to the nature and complexity of the organisation's business – for example, some businesses deal only with corporate customers and do not collect or use any meaningful level of personal data, and may thus be considered to be significantly lower risk from a personal data compliance perspective.

25 Based on the considerations above, an organisation should be able to choose:

- (a) whether the DPO appointment itself should be filled internally or externally; and
- (b) even if the DPO is internal, whether some training, tools, aids or services may be procured externally to support the DPO.

III. A DPO's role, and how an outsourced DPO may approach certain points differently

26 A new DPO would typically wish, at the start of his appointment, to undertake an initial assessment of the organisation's business from a personal data protection perspective. Indeed, this is often where the "heavy lifting" lies. The key processes involved would include:

- (a) interviews with key stakeholders in the organisation, including the chief executive and senior management, key data and process owners, compliance specialists, legal department, human resources, IT, *etc*;
- (b) reviewing the key documentary records, including:
 - (i) the internal and external data protection policies of the organisation;
 - (ii) its record of data and process inventories, activities and flows; and
 - (iii) information on the geographical location of data and processing;
- (c) considering the need to review other relevant documents, including:

- (i) contracts with data intermediaries;
- (ii) provisions in business contracts regarding personal data processing;
- (iii) standard-term employment contracts;
- (iv) business continuity plans;
- (v) information security policies;
- (vi) data breach procedures;
- (vii) schedule of analytics performed (if any);
- (viii) schedule of automated decision-making procedures employed (if any); and
- (ix) schedule of surveillance practices employed (if any).

27 In the authors' view, for any organisation that processes more than a minimal amount of personal data, having a data inventory and record of processing activities would be most invaluable and beneficial to the DPO and organisation (even though this is not mandatory by law), as it would, for example:

- (a) sort the organisation's data – which may sometimes otherwise be semi-structured or wholly unstructured;
- (b) identify where personal data (as opposed to non-personal data) is held;
- (c) facilitate the identification of data and process owners;
- (d) facilitate the identification of key risks and corresponding controls;
- (e) document the legal basis of processing;²⁴
- (f) document how personal data is stored and secured;
- (g) identify cross-border and domestic data transfer issues; and
- (h) better manage retention policy and help in formulating retention schedules and deciding on disposal methods.

24 In Singapore, notification and consent is the primary basis of processing, subject to specified exceptions in the Personal Data Protection Act 2012 (Act 26 of 2012). By contrast, in the European Union, for example, consent is only one of several bases of processing and in some cases (*eg*, in the employment context) valid consent may be difficult to secure. It is noted, however, that the Personal Data Protection Commission has consulted on (somewhat) expanding other bases of lawful processing besides consent.

28 In the event that key documentary records such as data protection policies and data and process inventories and flows are not available, the DPO may have to help produce them. In the case of a DPO from a service provider, however, it is likely that the service provider would wish to be engaged in its own right to perform this work *before* it agrees to accept an engagement to nominate a DPO.

29 Once the initial assessment is performed, a plan can be developed to remediate any gaps. One area where specialised expertise would be required would be in the field of information security practices.

30 On an ongoing basis, the organisation, with the DPO's involvement, would be expected to periodically review (or internally audit) aspects of its data protection management framework.

31 The matters referred to in paras 29 and 30 may be undertaken in-house or outsourced to the service provider or another third party.

32 Finally, as mentioned above, a key value-added role that a DPO can increasingly play beyond compliance is to use his data protection knowledge and his knowledge of an organisation's business operations and data processes to advise on how the organisation can still pursue business opportunities while staying within the law. It is often only the DPO that will have the knowledge and skills to be able to balance these various interests. In this way, the DPO can become more strategic, more senior and have a wider business role, as opposed to a simple legal compliance function. This is an area where an outsourced DPO can often play a useful role as he may have exposure to a wider array of data protection situations from work with other organisations or industry sectors.

USE OF DATA FOR BUSINESS IMPROVEMENT – BEYOND RIGHTS*

LEE Soo Chye

*LLB (Hons) (National University of Singapore),
MTax (Singapore University of Social Sciences);
Advocate and Solicitor (Singapore)*

TEO Yi Ting Jacqueline

*LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)*

Vera KOH Li Juen

*LLB (Hons) (University of Bristol);
Advocate and Solicitor (Singapore)*

I. Introduction

1 The Singapore Personal Data Protection Commission (“PDPC”) took bold initiatives in May 2019 to position Singapore as a “trusted data hub”.¹ One of the PDPC’s initiatives is the introduction of the proposed business improvement provision (previously referred to as the data innovation provision) in the PDPC’s third public consultation in the review of the Personal Data Protection Act 2012² (“PDPA”).³

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

1 Personal Data Protection Commission, “Media Release – Personal Data Protection Commission Introduces Three Initiatives to Strengthen Accountability Among Organisations and Encourage Data Innovation” (22 May 2019).

2 Act 26 of 2012.

3 Personal Data Protection Commission, “Public Consultation on the Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) (hereinafter “Third Consultation Paper”).

2 The business improvement provision, once enacted, will allow organisations to use personal data collected in compliance with the PDPA for purposes of (a) operational efficiency and service improvements; (b) product and service development; and (c) knowing customers better (collectively, “business improvement purposes”). Organisations are not required to notify individuals and seek their consent to *use* their personal data for these business improvement purposes. The PDPC clarified, however, that the obligation to notify and seek consent from individuals continues to apply for the *collection* and *disclosure* of personal data for the business improvement purposes.⁴ The PDPC also expressly stated that business improvement purposes do not extend to sending direct marketing messages to customers and organisations must obtain consent for sending direct marketing messages to customers.⁵

3 In addition, organisations can continue to use personal data for business improvement purposes even where individuals have withdrawn their consent for the use or disclosure of their personal data.⁶

4 Feedback was received by the PDPC after the launch of the third public consultation in May 2019. Organisations and individuals provided their feedback to the PDPC. Most of these organisations were in support of the business improvement provision, while a few of these individuals articulated their apprehension in placing their personal data in the hands of organisations for *bona fide* uses.

II. Empowering improvements and the potential for misuse

5 The future economy is a digital economy that is powered by big data. It is widely recognised that big data is critical in enabling the improvements in and transformation of businesses today, with its ability to increase efficiency and empower improvements and innovation, and is consequently immensely valuable to contributing to the growth of the economy. Studies indicate that the data analytics industry is central to the Singapore economy, contributing at least \$1bn each year, and the value of regional big data and business analytics services in the region is projected to reach

4 Third Consultation Paper, para 3.5.

5 Third Consultation Paper, para 3.6.

6 Third Consultation Paper, para 3.7.

\$37bn by 2022.⁷ Looking further offshore, the value of the European data economy was projected to increase to €739bn by 2020, representing 4% of the overall European Union's gross domestic product ("GDP").⁸

6 More often than not, big data contains personal data. Increasingly, personal data has become more valuable for businesses and can be easily collected and processed with technology.⁹ It is not surprising that in today's environment, the use of data plays a key part in decision-making by organisations.¹⁰ The use of data by organisations to improve and innovate (referred to in this article as business improvement projects) is advantageous to the economy as well as society in general, including the public sector such as health and environmental policies.¹¹

7 While data can be used for the greater good, it can also be misused for nefarious purposes. The business improvement provision not only brings with it the promise of public good and advancement that can be achieved with innovation and improvements, but also a real risk of organisations misusing personal data under the guise of improvement.

8 Nonetheless, this does not mean that the use of data by organisations to improve and innovate is incompatible with data protection. Business improvement projects can only be scaled with a large pool of personal data. This pool of personal data can only be generated when consumers view their data as secured. However, consumers may be reluctant to provide their personal data, preferring to reduce or limit their digital footprint. With the increasing consumer awareness of the value of their personal data, coupled with the reports of allegations of data breaches and data misuse by established companies involved in the data industry such as Facebook and Google,¹² consumers are put on high alert and there is rising distrust of

7 Economic Development Board of Singapore, "Singapore's Big Ambitions for Big Data in 2019" (23 October 2018).

8 IDC & Open Evidence, "Final Report of the European Data Market SMART 2013/0063 Study" (1 February 2017).

9 Hannah Yee Fen Lim, *Data Protection in the Practical Context – Strategies and Techniques* (Academy Publishing, 2017) at p 2.

10 Third Consultation Paper, para 3.1.

11 Ed Stacey, "Data Privacy Laws Need Rethinking to Encourage Innovation" *Forbes* (7 June 2019).

12 "Australian Regulator Files Privacy Suit Against Google Alleging Location Data Misuse" *Channel NewsAsia* (29 October 2019); Jonathan Browning &

(continued on next page)

organisations in handling personal data. Further, unlike tangible property, personal data, once released or disclosed, cannot be recovered.¹³ The harm associated with the mishandling and misuse of personal data is extremely wide and includes both tangible (*eg*, financial loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality and other economic or social disadvantages) and intangible (*eg*, dignity of and respect for the person), and potentially broader societal harm (*eg*, erosion of societal values and accepted cultural values).¹⁴ Thus, if the business improvement provision is introduced as law, it is important for organisations to be aware of and mitigate such potential risks.

III. Personal Data Protection Commission’s initiatives in protecting data and fostering trust

9 That said, an emphasis on individuals’ rights to their personal data is by no means the only or best way to ensure the security of data and gain the trust of consumers, especially in today’s data-driven environment. Instead, consumers’ trust could be more easily earned, and data could be better secured, through the actions and accountability of organisations and the active enforcement by regulators. The PDPC’s notable initiatives in recent years demonstrate firm steps in this direction.

10 Recognising that building the accountability of an organisation must start from its management and employees, the PDPC developed the Data Protection Officer (“DPO”) Competency Framework and Training Roadmap (“DPO Framework”). The PDPC’s intention is for the DPO Framework to serve as a guide to helping data protection professionals increase their competencies – through setting out a clear career development path and identifying relevant training courses – in order to be better able to put into operation and use an organisation’s data protection policies and processes, and as a guide for organisations to hire the right data

Ellen Milligan, “Google Faces iPhone Privacy Lawsuit After Court Reinstates Case” *Bloomberg* (2 October 2019).

13 Hannah Yee Fen Lim, *Data Protection in the Practical Context Strategies and Techniques* (Academy Publishing, 2017) at p 7.

14 Hannah Yee Fen Lim, *Data Protection in the Practical Context Strategies and Techniques* (Academy Publishing) at p 17.

protection professionals.¹⁵ The empowerment of data protection professionals who have capabilities suited to their organisations in turn contributes towards good data protection practices which can inspire consumer trust.

11 The PDPC had also launched the Data Protection Trustmark (“DPTM”) Certification, which is administered by the Info-communications Media Development Authority (“IMDA”). The DPTM is intended by the PDPC to be a “visible indicator that an organisation adopts sound data protection practices”,¹⁶ with certification requirements based on parameters such as relevance to international data protection standards and industry best practices. The IMDA has also been appointed as Singapore’s accountability agent for the Asia-Pacific Economic Cooperation (“APEC”) Cross Border Privacy Rules (“CBPR”) and Privacy Recognition for Processors (“PRP”) Systems certifications, which serve to facilitate accountable data transfers between participating organisations and across jurisdictions. Organisations that seek to obtain certification whether in the form of the DPTM or under the APEC CBPR or PRP Systems have to demonstrate good data protection practices and compliance with data protection rules and consumer trust will be more forthcoming with the regulator’s stamp of approval.¹⁷

12 In an effort to strengthen consumer confidence in the enforcement actions taken by the PDPC, the PDPC also published its *Guide on Active Enforcement* in May 2019. The guide “provides insight into the PDPC’s enforcement policy” by outlining how the PDPC handles data protection complaints, investigates incidents and decides on the types of enforcement actions that the PDPC undertakes in different circumstances, as well as explaining the principles considered by the PDPC in determining financial penalties imposed on organisations in breach of data protection rules.¹⁸

15 Personal Data Protection Commission, “DPO Competency Framework and Training Roadmap” (17 July 2019).

16 Personal Data Protection Commission, “Data Protection Trustmark”.

17 The authors are of the view that mandatory certification is the way forward. Their views are expressed in Lee Soo Chye, Teo Yi Ting Jacqueline & Sheam Zenglin, “Towards Codes and Certifications – The Protection of Personal Data in the Digital Age” [2019] PDP Digest 52.

18 Personal Data Protection Commission, *Guide on Active Enforcement* (22 May 2019).

In line with this objective is also the intended introduction of the mandatory requirement in the PDPA imposed on organisations to report to the PDPC and notify affected individuals when there is a data breach that is likely to result in significant harm to or impact on affected individuals.¹⁹ The mandatory data breach notification regime was proposed by the PDPC in its first public consultation in the review of the PDPA in 2017²⁰ (“First Public Consultation”), and was met with majority support from the public.²¹ The regime seeks to ensure that organisations are held accountable for data breaches, which will in turn preserve consumer trust in the long term.

IV. Going further to building trust and empowering improvements

A. Incorporating legal safeguards in the business improvement provision

13 The focus shifts back to the proposed business improvement provision, which places the burden of safeguarding individuals’ interests and personal data squarely on the shoulders of organisations. In this regard, the business improvement provision is similar to the proposed “legitimate interests” exception (initially referred to as “legal or business purpose”) albeit arguably narrower in scope, and the “notification of purpose” approach, both of which were proposed by the PDPC in the First Public Consultation.

14 The proposed “legitimate interests” exception was intended to permit organisations to collect, use or disclose the personal data of an individual without obtaining specific consent from that individual if there is a need to protect legitimate interests that will have economic, social, security or other

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

20 Personal Data Protection Commission, “Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (27 July 2017).

21 Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (1 February 2018) at para 7.2.

benefits to the public or a section of the public. The “notification of purpose” approach was intended to be a basis for organisations to collect, use and disclose individuals’ personal data where it is impracticable for the organisation to obtain consent and the collection, use or disclosure is not expected to have any adverse effect on the individuals. These suggested changes were described as “shifting the burden of responsibility from individuals to organisations to safeguard the interest of individuals”.²²

15 The same risks may arise in enacting the business improvement provision compared to an organisation’s reliance on the previously proposed “legitimate interests” exception and the “notification of purpose”. Guidance can therefore be taken from safeguards suggested by the PDPC to be put in place to mitigate risks if organisations rely on the “legitimate interests” exception or “notification of purpose” approach, such as the openness requirement²³ and the accountability measures.²⁴

16 Firstly, with regard to the openness requirement, an organisation should disclose its reliance on the business improvement provision as a ground for its use of individuals’ personal data, which could be done through an organisation’s data protection policy made available to the

22 Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (1 February 2018) at para 6.3.

23 The openness requirement refers to the requirement for an organisation relying on the “legitimate interests” exception to disclose its reliance as a ground for collection, use or disclosure of personal data and to make available a document justifying its reliance and the business contact information of a person who is able to answer questions about such collection, use or disclosure on behalf of the organisation. See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (1 February 2018) at para 5.9.

24 The accountability measures refer to the requirement for an organisation relying on the “legitimate interests” exception or the “notification of purpose” approach to collect, use or disclose personal data, to conduct a risk and impact assessment to identify and mitigate risks before reliance on these grounds to collect, use or disclose personal data. See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (1 February 2018) at paras 6.4 and 6.5.

public. The organisation should also make available a document that sets out justifications for an organisation's reliance on the business improvement provision and the business contact information of a person who will be able to address individuals' queries about such use by the organisation. Most would agree that an organisation that is transparent about what it is doing with the personal data it holds goes further in earning consumers' trust.

17 Secondly, in respect of the accountability measure, organisations should also document their use of individuals' personal data in reliance on the business improvement provision, for example, the types of personal data used, how the personal data will be processed by the organisation, and the purpose of doing so, as part of the documentation in the organisation's personal data asset register. This ensures that organisations can be held accountable as such records may be disclosed to the PDPC for consideration in determining whether there is any contravention of data protection rules in the event of complaints. These records can also be used by assessment bodies in their assessments of the organisation for the purposes of certifications such as the DPTM and the APEC CBPR/PRP that are tools to build confidence of consumers in organisations.

B Encouraging organisations' voluntary commitment to good data practices

18 Apart from the PDPC's initiatives, it is vital for organisations to consider putting in place certain practices to build trust with their customers or end users.

19 An example of such a practice is to collect less personal data and make optimal use of it.²⁵ Some organisations may be collecting more data than they need, which in turn results in their customers or end users raising questions and starting to have reservations about such organisations as they do not know what happens to their data.²⁶ In order for organisations to adhere to such a practice, the onus will be on organisations to decide which

25 Heidi Neumes, "Innovation vs Data Privacy or Innovation and Data Privacy?" *Digitalist Magazine* (17 July 2019).

26 Heidi Neumes, "Innovation vs Data Privacy or Innovation and Data Privacy?" *Digitalist Magazine* (17 July 2019).

type of personal data will be necessary or useful to them and only collect such personal data that is required.

20 Another suggestion is to encourage organisations to voluntarily provide a brief explanation to their customers or end users on how they intend to use the personal data collected for business improvement projects. This can be done by way of a notification poster or brochure, as Singapore Health Services Pte Ltd had recommended in its response to the Third Consultation Paper. Transparency builds trust – the more informed individuals are of what an organisation does to their personal data, the more likely they will trust that organisation to handle their personal data properly. If the business improvement provision is enacted as law without any safeguard requirements (as discussed above), an organisation’s commitment to such practices would be key to maintaining accountability and trust between it and its customers. In any case, organisations are required under the PDPA to develop and implement policies or practices to meet their obligations under the PDPA.²⁷

C Supporting organisations in innovation and improvements through a regulatory sandbox

21 The PDPC’s laudable efforts in supporting business improvement may also be supplemented by establishing regulatory sandboxes through which regulatory support can be provided. Singapore is no stranger to regulatory sandboxes – the Monetary Authority of Singapore implemented the FinTech Regulatory Sandbox in 2016 which “enables financial institutions and FinTech players to experiment with innovative financial products or services in a live environment but within a well-defined space and duration”.²⁸

22 This concept, specifically in relation to data protection, is currently being tested in the UK by the Information Commissioner’s Office (“ICO”). The ICO recognised a need for regulators to provide guidance and clarity on the practical application of data protection laws and regulation, in particular where organisations are exploring the use of personal data in

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

28 Monetary Authority of Singapore, “Overview of Regulatory Sandbox” (updated 7 August 2019).

exciting ways by using innovative technology. The ICO took steps to address this need by launching the beta phase of the ICO’s Sandbox in March 2019, through which it commits to providing expertise and support of the ICO to participating organisations on complying with the General Data Protection Regulation and the UK Data Protection Act 2018 in the process of developing innovative products and services, including assistance in concept design, prototyping and supervision of testing processes for such products and conducting workshops.²⁹

23 In fact, the PDPC has demonstrated its preparedness to work with organisations grappling with the proposed changes to the PDPA by creating regulatory sandboxes that will enable organisations to move faster, and at the same time, allow the PDPC to understand how the proposed changes to the PDPA might work in practice.³⁰ As with the UK, the PDPC may also consider going one step further by facilitating the development, by organisations, of innovative products and services from the use of personal data that offer public benefit, through regulatory sandboxes.

24 Such an alternative approach will not only directly enhance business improvement through use of data in Singapore, but also serve to foster better understanding of data protection rules within the organisation and bolster the organisation’s image of accountability in the public eye, leading to increased consumer trust.

V. Conclusion

25 On a grander scale, the business improvement provision, alongside the other robust initiatives undertaken by the PDPC such as the DPO Framework, the DPTM Certification, and the introduction of the mandatory breach notification regime, demonstrates an astute recognition of the necessity for the shift in focus of Singapore’s data protection framework from compliance with data protection rules and the enforcement of individuals’ rights to building trust and accountability between organisations and consumers.

29 UK Information Commissioner’s Office, “The Guide to the Sandbox (beta phase)”.

30 Personal Data Protection Commission, “Data Sharing Arrangements” (updated 26 March 2020).

26 Nevertheless, it is clear that to develop Singapore as a flourishing data hub in which consumers can put their trust and confidence, apart from strong regulatory support, there needs to be adequate legal safeguards and the robust commitment of organisations towards implementing good data protection practices.

**BEING ACCOUNTABLE IN TRANSFORMING YOUR
BUSINESS FOR DATA INNOVATION – LEARNING POINTS
FROM THE PERSONAL DATA PROTECTION
COMMISSION’S ENFORCEMENT DECISIONS IN 2019***

Steve TAN[†]

LLB (National University of Singapore),

LLM (University College London);

CIPP/A

Justin LEE[‡]

LLB (Singapore Management University)

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

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

‡ Senior Associate in Rajah & Tann Singapore’s TMT/Data Privacy practice group. In the course of his practice, Justin has advised clients on a wide range of transactional and regulatory matters with a particular focus on data privacy, intellectual property and technology law.

I. Introduction

1 The year 2019 saw the continued evolution of the data protection regulatory landscape in Singapore, with several noteworthy developments to Singapore data protection law taking place across the year. Viewed holistically, these developments highlight the overall regulatory approach that was adopted by the Personal Data Protection Commission (“PDPC”) in 2019 – and arguably still continues to be relevant in 2020 – with the PDPC recognising or acknowledging the delicate balance to be struck between encouraging greater data innovation by organisations with Singapore moving towards a transformative digital economy and the need for stronger accountability in the management of personal data by such organisations.

2 This regulatory approach was demonstrated in particular by the trio of initiatives that were concurrently launched on 22 May 2019 by the PDPC, which were collectively introduced with the specific aim of facilitating data innovation while strengthening accountability.

3 First, the PDPC issued a new public consultation as part of the ongoing review of the Personal Data Protection Act 2012¹ (“PDPA”), soliciting feedback on the proposed data portability and data innovation provisions that are proposed to be included in the PDPA (“Consultation Paper”). This was a direct follow-up from the “Discussion Paper on Data Portability” that had been issued by the PDPC in collaboration with the Competition and Consumer Commission of Singapore on 25 February 2019. The PDPC has generally received positive feedback in response to the Consultation Paper, and has since issued a response to the feedback received (“Response”).² Based on the Consultation Paper read together with the Response, the PDPC has proposed to introduce provisions into the PDPA that would (a) provide individuals with the right of data portability, which is a right that presently exists in some progressive data protection jurisdictions such as the European Union and the US state of California, by requiring organisations to transmit, at the request of the individual, his or her personal data that is in the organisation’s possession or control to

1 Act 26 of 2012.

2 Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) (hereinafter “Response”).

another organisation in a commonly used machine-readable format;³ and (b) permit organisations to use (but not collect or disclose) personal data without having to obtain the relevant individual's consent in respect of "business improvement" purposes comprising (i) operational efficiency and service improvements; (ii) product or service development; or (iii) knowing customers better.

4 Second, the PDPC published a new *Guide on Active Enforcement*,⁴ which sets out the PDPC's aim of deploying its regulatory powers in an effective and efficient manner when dealing with data breaches. The guide includes the introduction of a new expedited decision-making process that will allow the PDPC to swiftly conclude its investigation of non-controversial data breach cases, where the facts disclose a clear data breach and the investigated organisation is willing to provide an upfront admission of liability. Other conditions would apply, such as the organisation having to make a request for an expedited decision at the start of the investigation. The benefit of an expedited decision is that the organisation can have finality of the investigation in a short period of time as opposed to being under the yoke of an investigation for a prolonged duration. The guide also explains an alternative undertaking process, which organisations can consider proceeding with if the conditions of the factual matrix meet certain requirements. In this regard, an organisation that is being investigated can request the PDPC to allow it to proceed via this route of a voluntary undertaking being provided by the organisation in lieu of a full investigation by the PDPC, if that organisation can demonstrate to the PDPC that it has in existence robust internal accountability practices to comply with the PDPA and a sound remediation plan to deal with the breach that is being investigated. The organisation would then undertake to the PDPC that it will voluntarily remedy the breach and prevent its recurrence by executing its robust remediation plan. This process is generally only available to organisations which request it upon the commencement of investigations and/or in the early stages of an investigation. Hence, an organisation that has breached the PDPA and is

3 *Per* the Response, the Personal Data Protection Commission intends to prescribe the specific categories of personal data to which the data portability obligation will apply via codes of practice or other suitable regulatory instruments.

4 Published 22 May 2019.

the subject of an investigation by the PDPC would do well to consider at an early stage (such as when the data breach incident has occurred) whether it should request to initiate this undertaking process, and to seek the assistance of data protection law specialists in this regard if necessary.

5 Third, the PDPC published its *Guide to Managing Data Breaches 2.0*⁵ to provide organisations with greater clarity on how to manage data breaches more effectively, including an update on the thresholds and timelines for notifying the PDPC and/or affected individuals of a data breach. Each organisation is expected to have a data breach management plan in place, and to notify the PDPC and/or the affected individuals if the respective thresholds in question are met. The notification thresholds provide that an organisation would need to make a notification in the event of a data breach which affects 500 or more individuals, or where significant harm or impact to the affected individuals is likely to occur as a result of the breach.

6 The shift from compliance to accountability was also formally marked by the PDPC's issuance of its *Guide to Accountability under the Personal Data Protection Act* on 15 July 2019. This guide re-emphasises the importance of accountability in the modern digital economy, by replacing the Openness Obligation with the Accountability Obligation as one of the nine obligations under the PDPA. The principle of accountability provides for the mandatory need for each organisation to appoint at least one data protection officer,⁶ to have policies and practices to meet the PDPA requirements⁷ and the fact that each organisation is responsible for personal data within its possession or control.⁸

7 In conjunction with the foregoing, the PDPC has also provided regulatory and technical guidance on several other pertinent data protection issues in the course of 2019; for instance, the *Guide to Data Protection by Design for ICT Systems*,⁹ the *Guide to Developing a Data Protection Management Programme*¹⁰ and the *Guide to Notification*.¹¹

5 Published 22 May 2019.

6 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(3).

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

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(2).

9 Published 31 May 2019.

10 Updated 15 July 2019.

11 Updated 26 September 2019.

8 All of the developments discussed and summarised above underline the PDPC's continued efforts to impress on organisations the importance of pivoting from a culture of compliance to accountability in the management of personal data. This will allow organisations to provide the necessary degree of trust and confidence to their customers and other individuals whose personal data they possess or control, that such organisations have proactively identified and addressed risks to their personal data, thereby creating a solid foundation on which such organisations can safely leverage personal data in new and innovative ways.

9 The Data Protection Trustmark certification scheme, which was launched by the Infocomm Media Development Authority and the PDPC in January 2019, will continue to be one of the key methods by which certified organisations can visibly demonstrate their successful commitment to and implementation of the principles of accountability, thereby gaining a competitive advantage in respect of consumer trust and confidence. To date, 21 organisations in Singapore have successfully applied for and obtained Data Protection Trustmark certification. In conjunction with the foregoing, Singapore organisations which engage in data transfers across the Asia-Pacific region may also seek to be certified under the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules System and/or Privacy Recognition for Processors System, which will enable certified data controllers and data processors across the APEC region to exchange personal data more efficiently and seamlessly.

10 Given the continued importance of the need for strong accountability practices, organisations would do well to take guidance from the PDPC's enforcement decisions. This article will briefly discuss and highlight the key areas of guidance that can be extracted from some of the PDPC's enforcement decisions issued in 2019, in order for organisations to better understand the data protection practices that should be adopted pursuant to the PDPA's data protection obligations and better demonstrate their accountability in personal data protection.

II. Overview of the enforcement decisions issued by the Personal Data Protection Commission in 2019

11 Based on the number of enforcement decisions issued in 2019, the PDPC has significantly ramped up its PDPA enforcement efforts, with the number of reported decisions¹² almost doubling from 29 reported decisions in 2018, to 51 reported decisions in 2019. This increase may be partially attributable to the PDPC's expedited decision process (as set out in the *Guide on Active Enforcement*) described above,¹³ which has enabled the PDPC to efficiently resolve clear-cut data breach cases without having to go through a protracted period of investigation. The increase in the number of enforcement decisions is likely also representative of the increasing frequency of occurrence of data breach incidents in today's digital world.

12 As with previous years, the vast majority of the enforcement decisions in 2019 involved a finding by the PDPC that there had been a breach of the Protection Obligation under the PDPA by the organisation in question. Findings of breaches of the Accountability Obligation (previously referred to as the Openness Obligation) as well as the Consent and Notification Obligations were also present in the 2019 enforcement decisions. Where breaches of the PDPA were established by the PDPC after their respective investigations, the organisations in question were punished with financial penalties and/or directions for compliance, or in the case of less severe breaches, given warnings.

III. Key learning points

13 One of the key lessons that can be gleaned from the 2019 enforcement decisions is that organisations are expected to proactively identify, assess and mitigate the risks to personal data in their possession or control. It is evident from the 2019 enforcement decisions that the IT systems and processes being utilised by organisations in their processing of personal data are common sources of risk and vulnerability for personal

12 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 See para 4 above.

data. Such risks can only become more pronounced as organisations transform themselves operationally to embrace the digital economy.

14 The PDPC’s decision in *Re Singapore Health Services Pte Ltd*,¹⁴ which involved the exfiltration of the personal data of approximately 1.5 million patients of healthcare institutions within the Singapore Health Services Pte Ltd (“SingHealth”) healthcare cluster and has been described as “the worst breach of personal data in Singapore’s history”,¹⁵ is particularly instructive in this regard. In its decision, the PDPC reaffirmed the established principle set out in *Re Social Metric Pte Ltd*¹⁶ and other similar cases – where an organisation’s data processing activities have been outsourced to an 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.¹⁷

15 The PDPC found that SingHealth, as the primary organisation, had discharged its obligation of maintaining adequate oversight over the provision of IT operations and security services by Integrated Health Information Systems Pte Ltd (“IHIS”), SingHealth’s outsourced external vendor, through various levels of board, management and operational oversight and audit mechanisms. However, the PDPC found that one of the contributing causes of the data breach was the failure of a senior member of the SingHealth staff responsible for cybersecurity matters to properly escalate the incident to the appropriate channels upon being alerted of a possible cybersecurity breach. The PDPC noted that this failure was not only a failure by a single officer of SingHealth to discharge his responsibilities, but was symptomatic of a larger systemic issue with SingHealth’s organisational set-up, as the relevant employee did not have the resources or the technical and IT security expertise to properly fulfil his functions. This formed one of the bases on which the PDPC found that SingHealth had breached the Protection Obligation under the PDPA.¹⁸

14 [2019] PDP Digest 376.

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

16 [2018] PDP Digest 281.

17 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [57].

18 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [78]–[96].

16 On the part of IHiS, the PDPC found that IHiS had similarly breached the Protection Obligation under the PDPA by failing to take sufficient security steps or arrangements to protect the personal data it was processing on behalf of SingHealth from unauthorised access, collection, use, disclosure and copying. Security flaws identified by the PDPC included weak local administrator passwords, failure to disable dormant administrator accounts, and having an administrator password saved in unencrypted text within the server scripts.¹⁹

17 One key takeaway from the SingHealth enforcement decision is that having in place a detailed and comprehensive set of data protection policies and processes would not be sufficient if the organisation's personnel are ultimately unable to carry out or execute the aforesaid policies and processes. Training on such policies is therefore key. The lack of requisite technical expertise within an organisation's staff to manage its complex IT systems is no excuse. That said, with the publication of the PDPC's *Guide on Active Enforcement* in May 2019, the fact that an organisation had implemented comprehensive data protection policies and practices may now potentially allow the organisation to utilise the undertaking process, thereby enabling the organisation to avoid the cost and effort involved in dealing with a protracted investigation by the PDPC.

18 It is pertinent to note that one or more of the security flaws or issues that were identified in the IHiS IT systems or processes were similar to one or more of the security flaws or issues that had been identified as the causes of data breaches in previous PDPC enforcement decisions (such as in the cases of *Re Orchard Turn Developments Pte Ltd*,²⁰ *Re The Cellar Door Pte Ltd*²¹ and/or *Re K Box Entertainment Group Pte Ltd*²²). In this regard, it would be in the interest of organisations to take heed of decisions reported by the PDPC as the lessons from such decisions can help organisations avert a potential breach on their end.

19 In a similar vein, organisations should take note of the lessons in IT security practices that can be gleaned from the 2019 enforcement decisions. For organisations that store personal data on cloud servers (which

19 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [101]–[134].

20 [2018] PDP Digest 223.

21 [2017] PDP Digest 160.

22 [2017] PDP Digest 1.

the authors note is an increasingly ubiquitous practice), the decision in *Re Honestbee Pte Ltd*²³ highlights that organisations should not overlook the relatively simple step of ensuring that the personal data is stored in a “bucket” (ie, file folder) with appropriate access controls, given that cloud service providers do provide their customers with access to buckets with varying levels of access restrictions or security controls. Separately, the decision in *Re Learnaholic Pte Ltd*²⁴ demonstrates that personal data that is transmitted or stored in bulk should be transmitted or stored in encrypted form. Due care should also be taken to ensure that any modifications or reconfigurations to IT systems are not done in a manner that would create security vulnerabilities, whether as a result of a desire for convenience or otherwise. In this instance, Learnaholic had omitted to close a firewall security port that it had opened to enable convenient remote access to the IT system. Organisations should take note that, while it may not be possible to completely eliminate human error in every instance, carrying out security testing of the system for vulnerabilities after any changes to security system settings are made would help ensure that such human errors or omissions are not overlooked.

20 In this digital economy, many organisations deploy websites or online platforms to conduct business with their customers, and often engage third-party vendors to carry out the development and implementation work for their websites or online platforms. The case of *Re Horizon Fast Ferry Pte Ltd*²⁵ illustrates that the failure by an organisation to consider (or instruct its IT vendor to consider) data protection issues in the design of its online platform is a potential recipe for a data breach. Horizon Fast Ferry did not enter into a written contract with the vendor responsible for revamping its online platform, and thereby omitted to inform the vendor of its data protection obligations and to instruct the vendor to put in place proper safeguards to protect the personal data in the organisation’s possession or control. It instead chose to convey instructions in a piecemeal manner verbally or via WhatsApp, which would have led to confusion or lack of clarity regarding Horizon Fast Ferry’s exact requirements. This problem was exacerbated by Horizon Fast Ferry’s failure to conduct proper user acceptance tests before deploying the online platform – it is imperative that

23 [2020] PDP Digest 546.

24 [2020] PDP Digest 387.

25 [2020] PDP Digest 357.

before any transactional website goes live, it must have been tested and checked for vulnerabilities with the objective of ensuring that personal data that may be disclosed or accessed by authorised users of the website is adequately protected, pursuant to the PDPA's Protection Obligation.

21 Additionally, organisations that engage service providers located outside Singapore, including in relation to the storage of data or the hosting of websites or online platforms on overseas servers, should be mindful of the need to comply with the PDPA's Transfer Limitation Obligation in respect of all overseas transfers of personal data. Organisations should be at all times aware of where their service providers or their servers are located and should request for such information from their service providers if it is unclear. This was borne out in the cases of *Re Bud Cosmetics Pte Ltd*²⁶ and *Re Spize Concepts Pte Ltd*,²⁷ where the organisations involved were found not to have complied with the Transfer Limitation Obligation under the PDPA.

22 Ransomware is another threat that organisations are commonly facing today. The 2019 cases of *Re DS Human Resource Pte Ltd*,²⁸ *Re Genki Sushi Singapore Pte Ltd*,²⁹ *Re Marshall Cavendish Education Pte Ltd*³⁰ and *Re Chizzle Pte Ltd*³¹ all involved incidents of ransomware or ransom demands by hackers who had gained access to the organisation's personal data. It is therefore clear that organisations should be cognisant of this threat and take adequate technical and organisational measures to protect themselves against any form of ransomware attacks. This would include providing employees with the necessary data security training to recognise and not fall victim to phishing attacks, which is a common way in which malicious actors gain access to IT systems to install ransomware.

IV. Conclusion

23 This article has sought to highlight some of the notable lessons relating to data protection and accountability practices that can be observed

26 [2019] PDP Digest 351.

27 [2020] PDP Digest 311.

28 [2020] PDP Digest 274.

29 [2020] PDP Digest 347.

30 [2020] PDP Digest 425.

31 [2020] PDP Digest 506.

from the enforcement decisions issued by the PDPC in 2019. As with previous years, breaches of the Protection Obligation continue to be the main source of such lessons as many organisations fail to implement sufficiently robust technical and organisational security measures in the protection of personal data. It is hoped that organisations take heed of the problem areas identified in the PDPC's enforcement decisions and take steps to ensure that any similar security vulnerabilities that exist in their own systems and processes are addressed immediately. In doing so, organisations would better demonstrate their commitment to accountability in personal data protection, thereby gaining the confidence and trust of their customers and enabling the organisations to enjoy the competitive advantages associated with data innovation.

DATA PORTABILITY: STRIKING THE RIGHT BALANCE BETWEEN THE INDIVIDUAL AND “DATA CONTROLLER”*

Charmian AW†

LLB (Hons) (National University of Singapore);

CIPP/A, CIPP/E, CIPP/US, CIPM, FIP; Advocate and Solicitor (Singapore)

Cynthia O’DONOGHUE‡

BA (Arizona State University), LLM (University of Edinburgh),

JD (University of California, Davis School of Law);

Solicitor (England & Wales and Ireland); Member, New York Bar

Sarah BRUNO§

BS (Pennsylvania State University), JD (American University Washington College of Law);

CIPP/US; Admitted to District of Columbia, Maryland and California Bar; CIPP/A, CIPP/E, CIPM, FIP;

Advocate and Solicitor (Singapore)

1 Singapore is looking to adopt data portability as part of its efforts to drive data innovation and boost the overall development and

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

The reference to data controller is in quotation marks as it is not a term that is used in the Personal Data Protection Act 2012 (Act 26 of 2012) (“PDPA”). A data controller is typically an organisation that determines the means and purposes of processing personal data. A data processor processes that same data on behalf of the data controller. Both are mutually exclusive. In Singapore, however, an organisation is a broad category that encompasses both data controllers as well as data processors (or data intermediaries as referred to in the PDPA). Under the PDPA, an organisation is responsible for personal data in its possession or under its control (at s 11(2)), which covers a wider scope as compared to determining the means and purposes of processing.

† Counsel, Reed Smith, Singapore.

‡ Partner, Reed Smith, London.

§ Partner, Reed Smith, San Francisco.

competitiveness of our digital economy. Whilst the Personal Data Protection Act 2012¹ (“PDPA”) is being reviewed, it is critical that the new law must strike an appropriate balance amongst the interests of all the relevant stakeholders, *ie*, existing and new providers, consumers and other data subjects. This article seeks to highlight several key considerations to implementing data portability into Singapore law, as well as drawing potential comparisons with the European Union (“EU”) and California in scoping, interpreting and enforcing this complex but important right.

I. Proposed data portability under the Personal Data Protection Act 2012

2 In essence, data portability is the right individuals have to request organisations to transmit² data held about them to another service provider.

3 Whilst often regarded as an extension and complementary to the Access Obligation,³ since both are effectively consumer-initiated rights of request, portability is distinguishable from access in that it only applies to electronic data, and gives individuals the ability to move their data for the purposes of switching service offerings as opposed to merely being given information about how their data is being processed by an organisation.

A. Policy objectives

4 From a policymaking standpoint, there are a number of objectives to introducing portability into Singapore:

(a) **Consumer impact.** First, portability empowers individual consumers by giving them greater control over their personal data as well as facilitating their ability to opt for another service without hindrance.

(b) **Market impact.** Second, portability can be said to enhance competition by making it easier for businesses to tap a wider and

1 Act 26 of 2012.

2 Such transmission entails giving the receiving organisation a copy of the data as opposed to handing over the dataset in its entirety.

3 Personal Data Protection Commission, “Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at paras 2.42 and 2.43.

more varied pool of data, thereby generating efficiencies in the market. On the demand side, consumers may also be more motivated to try out new competitive products.

(c) **Economic impact.** Third, as portability expands the usability of the data and facilitates data access and innovation, this in turn encourages the promulgation of novel business ideas and product offerings. Hence portability has the potential to drive further growth and ensure Singapore stays relevant in the dynamic digital economy.

(d) **International cohesion.** Finally, it is important for Singapore to keep at the forefront of international data protection developments and standards. Data portability has already been introduced in the EU, the US (California), Australia and the Philippines. India, Japan and New Zealand are also considering the introduction of portability in their domestic laws.

5 Whilst there are compelling reasons for introducing this law, implementing portability requires a delicate balance amongst several interested stakeholders, namely, the consumer, other individuals whose data may be subject to porting obligations, the porting organisation, as well as competing businesses.

6 This article discusses the pertinent factors that were taken into account by the Personal Data Protection Commission of Singapore⁴ (“PDPC”) in considering this issue and the impact on interested parties arising from the new law.

B. Covered organisations

7 The first issue that was considered was which organisations would be subject to portability.

4 See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) which provides further clarity on the scope of the proposed Data Portability Obligation.

8 It was determined that organisations already subject to the obligations in the PDPA should rightfully be included,⁵ with the exception of data intermediaries.⁶

9 Also, the obligation will initially⁷ be limited such that organisations only need to transmit data to an entity that is formed or recognised under Singapore law or has a place of business in Singapore.⁸

C. Covered data

10 In relation to the type of data that would be subject to the portability requirement, only user-provided and user activity data⁹ of individuals that

5 This refers to any organisation that collects, uses or discloses personal data in Singapore, except for: (a) any individual acting in a personal or domestic capacity; (b) any employee acting in the course of his employment with an organisation; (c) any public agency; and (d) any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

6 A data intermediary is an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation. It was considered that data intermediaries should be excluded from the portability requirements because where an organisation engages a data intermediary to carry out processing of its data, it can enter into a contract and require the intermediary to assist with processing and responding to any portability requests on its behalf. The organisation itself should remain primarily responsible for complying with the Data Portability Obligation.

7 The Personal Data Protection Commission may subsequently issue regulations to extend the requirement to like-minded jurisdictions with comparable protection and reciprocal arrangements.

8 This will not prevent voluntary arrangements between organisations for the transmission of data from Singapore overseas, provided that the relevant individuals have given their consent.

9 “User-provided data” refers to personal data provided by an individual to an organisation; for instance, their contact details and personal preferences. “User activity data” refers to personal data about an individual that is created in the course or as a result of the individual’s use of any product or service provided by the organisation. See s 2(b) of the draft Personal Data Protection (Amendment) Bill 2020 (14 May 2020).

have a “direct and existing relationship”¹⁰ with the porting organisation, and which are in electronic format, would be covered. This is to take into account any potential impact portability could have on a business’s competitive position, and to recognise its proprietary input towards generating innovative product or service offerings¹¹ in the market.

11 Further, business contact information would be included in the Data Portability Obligation as there is value to both the individuals and receiving organisations for such data to be ported,¹² and no likely major impact to the porting organisation either. User-provided and user activity data of third parties may also be portable, where a request is made in the requesting individual’s personal or domestic capacity. This seems a sensible approach, since it would be impractical to obtain consent from all such third parties, or to redact their personal data when there is unlikely to be any adverse

10 As noted in Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020), it is unlikely that portability will pose any significant detriment to third parties’ personal data, provided that the receiving organisation provides for adequate protection of the data. Individuals today are able to disclose third-party data that they possess (*eg*, photographs, contact lists, *etc*) to any service provider, and to generate user-activity data that includes third parties’ data (*eg*, entering into transactions involving third parties). The processing of third parties’ personal data without consent by a receiving organisation will be allowed so long as that data is under the control of the requesting individual and used only for their own personal or domestic purposes, and not other purposes (*eg*, marketing).

11 See Personal Data Protection Commission, “Public Consultation on Review of Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at para 2.25.

12 The reason for this is that business contact information is provided by individuals to facilitate business activities, and allowing such individuals to port their data supports this objective of promoting business activities: see Personal Data Protection Commission, “Public Consultation on Review of Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at para 2.31.

effect to them for porting requests that are restricted to an individual’s personal or domestic capacity.¹³

12 Notably, only white-listed datasets prescribed in subsidiary legislation to be issued by the PDPC will be subject to the Data Portability Obligation in Singapore.¹⁴ Such subsidiary legislation will be issued incrementally in consultation with industry stakeholders, with a view to reducing compliance costs whilst providing clarity and certainty to businesses.

D. Exceptions

13 It is also relevant and necessary to weigh up the various stakeholders’ interests when considering the appropriateness of any applicable exceptions to the Data Portability Obligation. These exceptions will mirror those to the Access Obligation under the Fifth Schedule to the PDPA.¹⁵

14 A key exclusion that the PDPC determined would be required is in relation to any commercially sensitive or “derived” data.¹⁶ Having this exclusion would help safeguard against unfair competition by preserving

13 See Ministry of Communications and Information and the Personal Data Protection Commission, “Public Consultation on the Draft Personal Data Protection (Amendment) Bill” (14 May 2020) at para 46.

14 See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) at para 3.9; and Ministry of Communications and Information and the Personal Data Protection Commission, “Public Consultation on the Draft Personal Data Protection (Amendment) Bill” (14 May 2020) at para 47(a).

15 See Ministry of Communications and Information and the Personal Data Protection Commission, “Public Consultation on the Draft Personal Data Protection (Amendment) Bill” (14 May 2020) at para 48.

16 Derived data refers to personal data about an individual that is derived by an organisation in the course of business from other personal data about the individual or another individual in the possession or under the control of the organisation, but does not include personal data derived by the organisation using any prescribed means or method (which may include simple, non-proprietary algorithmic methods). See s 2(a) of the draft Personal Data Protection (Amendment) Bill 2020 (14 May 2020).

a business's commercial incentives and first-mover's advantage to develop and bring to market an innovative offering.¹⁷

15 Other exceptions include where the burden or expense of porting is unreasonable to the organisation or disproportionate to the individual's interests (for instance, where it is not technically feasible to port the data).¹⁸

E. Requesting individuals

16 Given that the premise of introducing portability is to give individuals greater control of their data, it is imperative that any obligation to port should only arise pursuant to a request made by that relevant individual. In addition, such requesting individual must also be the authorised party to the contract with the porting organisation for the provision of the product or service.¹⁹ This condition is intended to mitigate any risk of unauthorised porting requests being made on behalf of any individual.

F. Obligations of porting organisation

17 In terms of the scope of obligations that would be imposed on the porting and receiving organisations, once again this was carefully calibrated amongst the various stakeholders. In its "Response to Feedback on the

17 In its "Public Consultation on Review of Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions" (22 May 2019) ("22 May 2019 Consultation"), the Personal Data Protection Commission ("PDPC") emphasised that portability must not stifle business innovation by removing commercial incentives towards innovation. At the same time, the law must not preserve any first-mover advantage for a longer period than is appropriate, and hence the PDPC sought feedback on the relevant considerations in striking the right balance. See para 2.29 of the 22 May 2019 Consultation. Following its review of such feedback from the industry, the PDPC assessed that it would need to exempt from the portability requirement data that is commercially sensitive to a business, as well as any derived data.

18 See Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions" (20 January 2020) at para 3.10.

19 See Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions" (20 January 2020) at para 3.13.

Public Consultation on Proposed Data Portability and Data Innovation Provisions”, the PDPC assessed that porting organisations will not be required to allow individuals to verify the data before it is ported.²⁰ This is due to the fact that receiving organisations are already subject to the Accuracy Obligation in the PDPA and hence need to have policies and practices to ensure the ported data is accurate and complete if they are likely to use it to make decisions that affect the relevant individuals.

18 However, porting organisations may be required to preserve the relevant data minimally for 30 calendar days after porting, or rejecting a request, whichever is applicable. Retention by the porting organisation of the data beyond this period will depend on the circumstances, for instance, if there is a valid legal or business purpose for doing so or a continuing relationship with the individual in question.²¹

G. Obligations of receiving organisation

19 On the flip side, organisations that receive ported data will be regarded as having collected personal data and thereby subject to all of the obligations under the PDPA in respect of that data which is now in their possession or control.

20 Upon receiving the ported data, a receiving organisation should check that it can access such data, and that all data fields indicated by the requesting individual are complete. If it has any issue receiving or accessing the data, it should notify the porting organisation as soon as practicable,

20 Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) at para 4.9.

21 Organisations should be careful not to retain data “just in case” an individual were to make a porting request, as portability will not be an excuse for not complying with the Retention Limitation Obligation in the Personal Data Protection Act 2012 (Act 26 of 2012). See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) at para 4.13.

and the porting organisation should seek to address this within a reasonable period.²²

H. Practical implementation

21 The PDPC has clarified that the Data Portability Obligation would be implemented in phases and guided by subsidiary legislation, which would be developed in consultation with industry stakeholders. Such subsidiary legislation would cover the following:

- (a) “White-listed” datasets which would be the *only* data subject to the portability requirements. For instance, consumer spending history could include data on purchases and payments; and utilities consumption history could include data on mobile data usage and electricity utilisation. Any organisation holding such white-listed datasets, regardless of sector,²³ would need to comply with the Data Portability Obligation.
- (b) Any technical and process details for ensuring the correct data is ported securely to the correct receiving organisation, and in a usable format. These would include the porting time frame, data formats, transmission protocols, authentication protocols and cybersecurity standards, to enable interoperability between organisations porting and receiving the data.
- (c) Any preferred model for the porting. Consumers could either make the data porting request directly to the porting organisations (“push model”) or through the receiving

22 See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) at para 4.14.

23 As digital data is considered the currency that “powers” the digital economy, the ability to move such data within and across sectors is crucial to the growth of the digital economy (see Personal Data Protection Commission, “Public Consultation on Review of Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at para 2.23).

organisations (“pull model”).²⁴ These models would serve different scenarios or businesses.

- (d) Any additional safeguards customised based on the risks of the white-listed datasets; for instance, cooling-off periods to retract a porting request, and any blacklist that porting organisations may refuse to port data to. The consumer safeguards would be determined in consultation with the industry when developing the regulations.

22 At the time of writing, it was indicated²⁵ that any fees that a porting organisation could rightfully charge for acceding to a porting request could be set out in advisory guidelines to be issued in due course. To the extent that a porting organisation could conceivably incur costs to port data pursuant to a valid request, an assessment would need to be made as to how such costs could be allocated and then passed on to each of the requesting individuals and/or receiving organisations. It is anticipated that the PDPC would also have powers to review any refusal to port data pursuant to a relevant request, any failure to port data within a reasonable period, and any fees that could be charged for acceding to a porting request.

II. Data portability under the General Data Protection Regulation

23 The General Data Protection Regulation²⁶ (“GDPR”) provides a comprehensive framework for harmonised governance of data protection rules across the EU. The GDPR is a response to the technological advances since the Data Protection Directive²⁷ was implemented into national law.

24 An example of the pull model is when an individual wishes to use a new service. The new service provider explains to him the datasets required, how they will be used and where they can be ported from. The individual proceeds to authorise the new service provider (receiving organisation) to make the porting request on his behalf. The push model may be appropriate if there is an established industry practice for a standard set of data to be pushed to the receiving organisation.

25 See Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions” (20 January 2020) at para 4.11.

26 General Data Protection Regulation (EU) 2016/679 (entry into force 25 May 2018) (hereinafter “GDPR”).

27 95/46/EC.

The GDPR repealed the Data Protection Directive and became directly applicable in EU member states on 25 May 2018.²⁸ In a number of areas, EU member states can restrict, adapt and derogate from the GDPR and enact their own laws – for example, in the UK this is achieved by the Data Protection Act 2018.²⁹

A. Covered organisations

24 The GDPR applies to organisations that are based in the EU even if the data is being stored or processed outside of the EU.³⁰ It also applies to:

- (a) a company which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
- (b) a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU.³¹

This means that some non-EU businesses are required to comply with the GDPR.

B. Covered information

25 “Personal data” is broadly defined and includes information relating to natural persons who:³²

- (a) can be identified or who are identifiable, directly from the information in question; or
- (b) who can be indirectly identified from that information, in particular by reference to an identifier such as “a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

28 GDPR Art 94.

29 c 12.

30 GDPR Art 3(1).

31 GDPR Art 3(2).

32 GDPR Art 4.

26 The GDPR also has broad application and applies to personal data processed manually and electronically:

- (a) personal data processed wholly or partly by automated means (or information in electronic form); and
- (b) personal data processed in a non-automated manner which forms part of, or is intended to form part of, a “filing system” (or written records in a manual filing system).

This means that the GDPR protects personal data regardless of the technology used for processing that data as it applies to both automated and manual processing.

27 The definition of personal data is also important as only personal data is in the scope of a data portability request. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been anonymised in such a way that the individual is no longer identifiable is not considered personal data. The anonymisation must be irreversible.

C. *Right to data portability*

28 The right to data portability is one of eight rights enforced by the GDPR.³³ The purpose of this right under the GDPR is to empower data subjects and give them more control over their personal data as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another.³⁴

33 The other GDPR rights for individuals include the: right to be informed, right of access, right to rectification, right to erasure (also known as “the right to be forgotten”), right to restrict processing, right to object and rights in relation to automated decision-making and profiling. See generally Arts 12–23 of the GDPR.

34 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at pp 1 and 4.

29 The principle of data portability is set out in Art 20 of the GDPR:³⁵

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided ...

30 Under the GDPR, data portability: (a) is a right of the data subject to receive a subset of the personal data processed by a data controller concerning him, and to store those data for further personal use; which (b) provides the data subject with the right to transmit personal data from one data controller to another data controller.³⁶

31 In accordance with Art 20(1)(a) of the GDPR, in order to fall under the scope of data portability, processing operations must be based either:

- (a) on the data subject's consent (pursuant to Art 6(1)(a) of the GDPR, or pursuant to Art 9(2)(a) of the GDPR when it comes to special categories of personal data); or
- (b) on a contract to which the data subject is a party pursuant to Art 6(1)(b) of the GDPR.

This is because compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data. The GDPR does not establish a general right to data portability where the processing of personal data is not based on consent or contract.³⁷

D. Facilitating a request

32 The GDPR does not specify how data subjects should make data portability requests. Requests could be made orally or in writing. They can also be made to any part of the organisation as opposed to a particular data

35 GDPR Art 20.

36 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at pp 4–5.

37 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 8. See also Recital 68 of the GDPR and Art 20(3) of the GDPR.

privacy contact point. A valid data portability request does not have to include the phrase “request for data portability” or a specific legal provision to be valid. As such, it is recommended that organisations give specific training on recognising a request to staff members who regularly interact with data subjects.

33 Additionally, it is good practice under the GDPR to:

- (a) have a policy in place for recording details of the requests received;
- (b) check with the requester to make sure the request is clearly understood, which can help avoid later disputes about how the controller interpreted the request; and
- (c) keep a log of all requests (written or otherwise).

34 There are no prescriptive requirements found in the GDPR on how to authenticate the data subject. If there are any doubts about the identity of the data subject making the request, organisations should ask for information that is necessary to confirm the data subject’s identity.³⁸ The key to this is proportionality. The organisation needs to let the data subject know as soon as possible that it needs more information from him to confirm his identity before responding to the request. The period for responding to the request begins when the organisation receives the additional information, if requested, and if not, the period starts when the data subject makes the request.

E. Obligations of porting organisation

35 Organisations answering data portability requests will be data controllers for the purposes of the GDPR. Under the conditions in Art 20 of the GDPR, those porting organisations are not responsible for the processing handled by the data subject or by the receiving organisation.

36 The porting organisation should set safeguards to ensure that the types of personal data transmitted are those that the data subject wants to

38 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 13.

transmit.³⁹ This could be done by obtaining confirmation from the data subject.

37 Organisations have no specific obligations to check and verify the quality of the data before transmitting it.⁴⁰ However, the organisation should already have the data accurate and up to date, according to the principles set out in Art 5 of the GDPR.

(1) *Time limit imposed to answer a portability request*

38 Organisations under Art 12(3) of the GDPR are required to answer a portability request “without undue delay” and in any event “within one month of receipt of the request”. The one-month period can be extended by two more months where necessary, taking into account the complexity and number of the requests, provided that the data subject has been informed about the reasons for such delay within one month of the original request.⁴¹

(2) *Cases in which a data portability request can be rejected or a fee charged*

39 There may be legitimate reasons why an organisation cannot undertake a transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is, however, the responsibility of the organisation to justify that these reasons are legitimate and not a “hindrance” to the transmission. Organisations who refuse to answer a data subject’s portability request should inform the data subject of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy, no later than one month after receiving the request.⁴²

39 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 6.

40 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 6.

41 GDPR Art 12(3).

42 GDPR Art 12(4).

40 No fee should be charged for the provision of personal data, unless the organisation can demonstrate that the requests are manifestly unfounded or excessive.⁴³ The Working Party paper on data portability suggests that the overall cost of the process created to answer data portability requests should not be taken into account to determine the excessiveness of a request.⁴⁴

(3) *Providing the portable data*

41 Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller or organisation “without hindrance” from the controller to which the personal data has been provided. This means that organisations should not erect any legal, technical or financial obstacles which slow down or prevent the request from being carried out.

42 There is no obligation to retain personal data beyond the otherwise applicable retention period to serve any potential future data portability request.

43 If a valid request for data portability is received, all steps to ensure compliance must be taken. Organisations can achieve this by either:

- (a) directly transmitting the requested data to the individual; or
- (b) providing access to an automated tool that allows the individual to extract the requested data themselves.

44 Where the data subject requests the organisation to transmit his personal data directly to another organisation, the organisation holding the personal data must comply if it is “technically feasible” to do so.

45 The technical feasibility must be considered on a request by request basis. Recital 68 of the GDPR further clarifies the limits of what is “technically feasible”, indicating that “it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible”.

43 GDPR Art 12(5).

44 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 15.

(4) *Expected data format*

46 The personal data should be provided in a format that is “structured”, “commonly used” and “machine readable”.⁴⁵ These terms are not defined in the GDPR.

47 Organisations are also required to consider the format to be used. The GDPR suggests, but does not require, organisations to use an interoperable format. Interoperability allows different systems to share information and resources. Recital 68 of the GDPR provides that “data controllers should be encouraged to develop interoperable formats that enable data portability”. The European Data Protection Board (“EDPB”) stresses that interoperability and not compatibility of systems is the key outcome.⁴⁶

(5) *Securing portable data*

48 The organisation is responsible for the transmission of the data and must ensure that it is transmitted securely⁴⁷ and to the right destination. Organisations should assess the specific risks linked with data portability and take appropriate risk mitigation measures. EDPB suggests that such risk mitigation measures could include additional authentication information, one-time password, suspending or freezing the transmission if

45 Recital 21 of Directive 2013/37/EU defines “machine readable” as:

... a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.

46 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 17.

47 Article 5(1)(f) of the GDPR provides that data controllers should guarantee the “appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”.

there is suspicion that the account has been compromised and using token-based authentications.⁴⁸

49 However, once the data is provided to the data subject or another organisation, the porting organisation is not responsible for any subsequent processing.

F. Obligations of receiving organisation

50 Organisations that receive ported data will be regarded as having collected personal data. As such, the receiving organisation becomes a new data controller and the ported data will need to be processed in line with the GDPR obligations and the principles stated in Art 5 of the GDPR such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, integrity and confidentiality, storage limitation and accountability.

51 In deciding whether to accept and retain the personal data, the organisation should consider whether the data is relevant and not excessive in relation to the purposes for which it will be processed. Any data received which is unconnected to the purpose of the new processing should be deleted and not processed.

52 As a new data controller, the organisation must ensure it has one or more lawful bases for processing any third-party data, and that this processing does not adversely affect the rights and freedoms of those third parties.

III. Data portability under the California Consumer Privacy Act

53 In the US, the concept of data portability was formalised into a right more recently in California, when the California Consumer Privacy Act of 2018⁴⁹ (“CCPA”) came into effect. The CCPA came into effect on

48 Article 29 of the Data Protection Working Party, now European Data Protection Board, *Guidelines on the Right to Data Portability*. Adopted on 13 December 2016 as last revised and adopted on 5 April 2017, at p 19.

49 Civil Code of the State of California (Title 1.81.5) §§1798.100–1798.199 (hereinafter “California Civil Code”).

1 January 2020 and is considered one of the most expansive US privacy laws to date.

A. Covered organisations

54 The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds:

- (a) has annual gross revenues in excess of US\$25m;
- (b) buys or sells the personal information of 50,000 or more consumers or households; or
- (c) earns more than half of its annual revenue from selling consumers' personal information.⁵⁰

B. Covered information

55 "Personal information" is broadly defined as any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".⁵¹ Examples of personal information include a consumer's name, mailing address, e-mail address, driver's licence number, state identification number, passport number, physical description, social security number, telephone number, insurance policy information, bank account number, credit/debit card number or any other financial information.

56 The statute excludes from the definition of personal information "publicly available information", which is information that is lawfully made available from federal, state or local government records.⁵² The statute also excludes from the definition of personal information the following categories: (a) protected health information collected by a covered entity as defined under federal laws including the Health Insurance Portability and Accountability Act; (b) the sale of information to or from a consumer reporting agency for use in a consumer report consistent with the Fair

50 California Civil Code §1798.140(c).

51 California Civil Code §1798.140(o)(1).

52 California Civil Code §1798.140(o)(2).

Credit Reporting Act; and (c) personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (“GLBA”) or the Driver’s Privacy Protection Act of 1994, to the extent the CCPA conflicts with those laws.⁵³

C. *Rights granted to consumers*

57 The rights under the CCPA are granted to “consumers” who are natural persons that are California residents.

D. *Rights granted by the California Consumer Privacy Act*

58 In addition to the right to data portability, the CCPA grants consumers several other rights, including the right to know what information is collected about them,⁵⁴ the right to request their information be deleted,⁵⁵ and the right to opt out of the sale of personal information.⁵⁶ The CCPA grants a right to equal service, prohibiting discrimination against consumers who exercise their rights.⁵⁷

E. *Right to data portability*

59 The CCPA states that a business that receives a “verifiable” request from a consumer to access their personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information.⁵⁸ Notably, the CCPA states that the information may be delivered by mail or electronically.

53 California Civil Code §§1798.145(c), 1798.145(d), 1798.145(e) and 1798.145(f).

54 These information access rights are scattered throughout the California Consumer Privacy Act of 2018, in §§1798.100(a), 1798.110(a) and 1798.115(a).

55 California Civil Code §1798.105(a).

56 California Civil Code §1798.120(a).

57 California Civil Code §1798.125.

58 California Civil Code §1798.100(d).

F. Facilitating a request

60 There are two steps to compliance with a request for data. The first is to “verify” the consumer is who they say they are. Businesses must establish, document and comply with a reasonable method for verifying requests. Whenever feasible, the business shall match the identifying information provided by the data subject to the personal information of the data subject already maintained by the business. The business should always avoid collecting sensitive information such as social security number, driver’s licence number, financial account information, medical information or health insurance information when verifying identity. In general, where there is sensitive or valuable personal information and/or a high likelihood that fraudulent or malicious actors will seek the personal information, a more stringent verification process will be warranted.⁵⁹

61 Once verified, the business can then provide the consumer with the information they requested. This may be done by mail or electronically. If electronically, it must be in a readily usable format that allows the consumer to transmit the information to another entity. There is currently no guidance on what is considered “technically feasible” or “readily useable”, but businesses can look to Art 20 of the GDPR for guidance. Article 20 provides for the data to be in a “structured, commonly used and machine-readable format” and also provides for direct transmissions from one controller to another upon request “where technically feasible”. The California Attorney General’s final regulations, when issued, may make mention of this language and data portability in general.⁶⁰

62 The proposed regulations state that if a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled

59 California Civil Code §1798.185, as further clarified by §999.323 of the Proposed Text of Regulations of the California Consumer Privacy Act Regulations.

60 On 10 October 2019, the California Attorney General announced proposed regulations implementing the California Consumer Privacy Act of 2018. The final regulations are expected on or before 1 July 2020.

to under the CCPA, uses reasonable data security controls, and complies with the verification requirements.⁶¹

IV. Comparison table

63 A snapshot comparison of the Data Portability Obligation and associated key requirements as proposed in Singapore, as well as under the GDPR and CCPA, can be found in the table below.

Relevant consideration	Singapore PDPA	EU GDPR	California CCPA
Covered organisations	<ul style="list-style-type: none"> Porting organisations can be any organisations that are subject to the PDPA, regardless of sector, but excluding data intermediaries. Initially at least, receiving entities must be formed or recognised under Singapore law or have a place of business in Singapore. 	<ul style="list-style-type: none"> Organisations based in the EU. Organisations which process personal data as part of the activities of one of their branches established in the EU, regardless of where the data is processed. Organisations established outside the EU which offer goods/services or monitor the behaviour of individuals in the EU. 	<ul style="list-style-type: none"> A covered entity is one that: <ol style="list-style-type: none"> handles “personal information” about California residents; alone, or jointly with others, determines the purposes and means of processing of that “personal information”; and does business in California. Most of the CCPA’s obligations apply directly to businesses that meet one of the following threshold requirements: <ol style="list-style-type: none"> has annual gross revenues in excess

61 Proposed Text of Regulations of the California Consumer Privacy Act Regulations §999.313(c)(7).

			<p>of US\$25m; (ii) annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information regarding at least 50,000 consumers, households or devices; <i>or</i> (iii) derives 50% or more of its annual revenue from selling personal information.⁶² In the context of car dealerships, this means that a family of dealerships may be viewed as one business.</p>
<p>Covered data</p>	<ul style="list-style-type: none"> • Only white-listed datasets prescribed in legally binding codes of conduct. • User-provided or user activity data, in electronic format, where requesting individuals have 	<ul style="list-style-type: none"> • Information relating to natural persons: • who can be identified, or who are identifiable, directly from the information in question; or • (b) who can be indirectly identified from 	<ul style="list-style-type: none"> • “Personal information” which is broadly defined as any “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular

62 California Civil Code §1798.140(c).

	<p>a “direct and existing relationship” with the porting organisation.</p> <ul style="list-style-type: none"> • Business contact information. 	<p>that information, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>	<p>consumer or household”.⁶³ Examples of personal information include a consumer’s name, mailing address, e-mail address, driver’s licence number, state identification number, passport number, physical description, social security number, telephone number, insurance policy information, bank account number, credit/debit card number or any other financial information.</p>
Exceptions	<ul style="list-style-type: none"> • Data collected pursuant to an exception to consent in the PDPA. • Confidential commercial or derived data. • Burden or expense of porting 	<ul style="list-style-type: none"> • Publicly available information. • Personal data that has been anonymised in such a way that the individual is no longer identifiable. • Burden or expense of 	<ul style="list-style-type: none"> • Publicly available information, which is information that is lawfully made available from federal, state or local government records.⁶⁴ • To the extent the CCPA conflicts

63 California Civil Code §1798.140(o)(1).

64 California Civil Code §1798.140(o)(2).

	unreasonable or disproportionate to requesting individual’s interests.	porting unreasonable or disproportionate to requesting individual’s interests.	with the following laws: ⁶⁵ <ul style="list-style-type: none"> • Protected health information collected by a covered entity as defined under federal laws including the Health Insurance Portability and Accountability Act. • The sale of information to or from a consumer reporting agency for use in a consumer report consistent with the Fair Credit Reporting Act. • (c) Personal information collected, processed, sold or disclosed pursuant to the GLBA or the Driver’s Privacy Protection Act of 1994.
Requesting individuals	<ul style="list-style-type: none"> • Must have direct customer relationship with porting organisation. 	<ul style="list-style-type: none"> • Natural persons (data subjects) whose data is held by the porting organisation. 	<ul style="list-style-type: none"> • “Consumers” who are natural persons that are California residents.

65 California Civil Code §§1798.145(c), 1798.145(d), 1798.145(e) and 1798.145(f).

<p>Obligations of porting organisation</p>	<ul style="list-style-type: none"> • Comply with legally binding codes of conduct and advisory guidelines. • Preserve the relevant data for 30 calendar days minimally after porting or rejecting a request, whichever is applicable. • Rectify within a reasonable time any access issues with ported data as may be notified by receiving organisation. 	<ul style="list-style-type: none"> • Authenticate data subject, if necessary. • Comply with GDPR obligations as a data controller. • Answer data portability request without undue delay and, in any event, within one month of receipt of the request (this period can be extended by a further two months). • If data portability request is rejected, inform the data subject of the reasons for not taking action and on the possibility of lodging a complaint with supervisory authority and seeking a judicial remedy. • No obligation to retain personal data beyond the otherwise applicable retention period. 	<ul style="list-style-type: none"> • Provide notice to consumers of their rights. • Provide two or more methods for the data subject to contact the business with a request to know, including an interactive webform accessible through the business’s website or mobile application. Other acceptable methods include, but are not limited to, a toll-free telephone number, designated e-mail address or form submitted through the mail. • Confirm receipt of the request within ten days and provide information about how the business will process the request, including the process for verifying the identity of the person making the request and when the consumer may expect a response. • Respond in substance within
--	--	--	---

		<ul style="list-style-type: none">• Directly transmit the requested data to the individual or provide access to an automated tool that allows the individual to extract the requested data himself.• Provide the data in a format that is structured, commonly used and machine-readable.• Transmit data securely and to the right destination.	<p>45 days; the 45-day period will start on the day the business receives the request, regardless of any time spent verifying the request; a business may take an additional 45 days if necessary so long as it has notified the consumer of the need for the additional time.</p> <ul style="list-style-type: none">• Must not at any time disclose a consumer's social security number, driver's licence number or other government issued identification numbers, financial account numbers, an account password or security question or health insurance or medical identification numbers.• Use reasonable security measures when transmitting the personal information to the consumer.
--	--	---	--

<p>Obligations of receiving organisation</p>	<ul style="list-style-type: none"> • Comply with the PDPA in respect of ported data received • Check that it can access the data ported and requested data fields are complete. If it has any issue receiving or accessing the data, it should notify the porting organisation as soon as practicable. 	<ul style="list-style-type: none"> • Comply with the GDPR in respect of ported data received. • Consider whether the data received is relevant and not excessive in relation to the purposes for which it will be processed. • Ensure the receiving organisation has one or more lawful bases for processing any third-party data, and that this processing does not adversely affect the rights and freedoms of those third parties. 	<p>N/A</p>
<p>Practical implementation issues: processes, timelines, porting mechanisms, fees to be charged, <i>etc.</i></p>	<ul style="list-style-type: none"> • To be prescribed in codes of conduct and advisory guidelines. 	<ul style="list-style-type: none"> • Authenticate data subject, if necessary. • Implement a policy and a log for recording details of requests received. • Answer portability requests without undue delay and in any event within one 	<p>See above on “Obligations of porting organisation”.</p>

		<p>month of receipt of the request (this can be extended by two further months).</p> <ul style="list-style-type: none">• No fee should be charged, unless the request is manifestly unfounded or excessive.• Personal data to be provided in a format that is structured, commonly used and machine-readable.	
--	--	--	--



DATA LOCALISATION: THE WAY FORWARD OR BACKWARD FOR DATA INNOVATION?*

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)*

Joshua KOW[‡]

*LLB (Hons) (National University of Singapore);
CIPP/A, CIPP/E, CIPM, FIP;
Advocate and Solicitor (Singapore)*

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

† Data Privacy Senior Counsel, ByteDance Ltd; Adjunct Law Lecturer, Singapore Management University School of Law; and Adjunct Assistant Professor, National University of Singapore Faculty of Law. Lanx was formerly the Head of Investigation with the Singapore Personal Data Protection Commission and Senior Legal Counsel, Privacy & Cybersecurity Lead, and Global Data Protection Officer with Klook Travel Technology Limited. He is a member of the Law Society's Cybersecurity and Data Protection Committee, one of the authors of *Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018), and has spoken at various conferences such as Data Protection in the Digital World Summit, Bulgaria 2019, FTI/HKACC: In-House Counsel: An Integral part of Cybersecurity, IAPP Asia Privacy Forum, and ISCA: Financial Forensic and Cybersecurity.

‡ Legal Counsel, Klook Travel Technology Limited.

I. Introduction

1 It is a widely accepted fact that, in many technologically driven economies and societies, data is a pivotal impetus for innovation. In a recent public consultation, the Personal Data Protection Commission of Singapore (“PDPC”) noted that “[t]he modern business marketplace is very much a data-driven environment, where data is at the core of almost every business decision made”.¹ Research by McKinsey Global Institute and McKinsey’s Business Technology Office also shows that “analyzing large data sets – so-called big data – will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus”.²

2 Closely related to data innovation is the need to share data. Often discussed together, the intertwined relationship between data innovation and data sharing is well documented in many industries, such as healthcare.³ In recent years, regulators have introduced various mechanisms to ensure that data can flow between industry players for the ultimate benefit of the consumer; for example, the right to data portability introduced under the General Data Protection Regulation⁴ (“GDPR”).

3 While recognising the need to drive data innovation, regulators are also cognisant of the other extreme – how unrestrained sharing of data could lead to abuse, especially in countries with weaker protections for personal data. This is especially considering how data innovation has become an increasingly transnational affair. With the explosion of cloud computing and the Internet of Things (“IoT”), a software-as-a-service (“SaaS”) business in Singapore could, for example, be operating on cloud infrastructure physically located in the US, or collecting personal data from European citizens through wearable IoT devices which are subsequently

1 Personal Data Protection Commission, “Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at para 3.1.

2 James Manyika *et al*, “Big Data: The Next Frontier for Innovation, Competition, and Productivity” *McKinsey Global Institute* (May 2011).

3 Claire Biot *et al*, “Data Sharing is Key to Innovation in Health Care” *MIT Technology Review* (27 September 2019).

4 General Data Protection Regulation (EU Regulation 2016/679) (entry into force on 25 May 2018) (hereinafter “GDPR”) Art 20 (right to data portability).

transferred to a Singapore-hosted server for analysis. This has led to the creation of requirements designed to limit, if not prohibit altogether, the transfer of personal data from one country to another. These range from flexible requirements which oblige a transferring organisation to ensure a comparable standard of protection⁵ prior to transfer, to broad-brush prohibitions on storing data anywhere outside a country's physical geographical boundaries.⁶

4 On the one hand, such requirements can be said to maintain data integrity and accuracy, protect the personal data of individuals, and ensure that national security is not threatened. On the other hand, companies which largely depend on cross-border data flows for innovation now have to wrestle with vagueness in the law, increased compliance costs, technological workarounds, and longer innovation cycles for new products and services. In the latter instance, the law stifles, instead of enables, data innovation.

5 The impact of data localisation requirements on world trade at a macroeconomic level has been discussed by, *inter alia*, various organisations and authors including the United Nations Conference on Trade and Development,⁷ Han-Wei Liu⁸ and Benjamin Wong.⁹ This article does not seek to do the same. Instead, this article focuses on comparing the various types of data localisation requirements present in various jurisdictions, and how they respectively affect the ability of organisations and businesses to innovate and compete in the digital economy.

5 For example, the Transfer Limitation Obligation stated at s 26 of the Personal Data Protection Act 2012 (Act 26 of 2012).

6 For example, Art 37 of China's Cybersecurity Law (effective 1 June 2017).

7 United National Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (United Nations, 2016 Ed).

8 Han-Wei Liu, "Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism" in *ASEAN Law in the New Regional Economic Order, Global Trends and Shifting Paradigms* (Pasha L Hsieh & Bryan Mercurio eds) (Cambridge University Press, 2019).

9 Benjamin Wong, "Data Localization and the ASEAN Economic Community" (2020) 10(1) *Asian Journal of International Law* 158.

II. Data localisation requirements – A comparative view

6 Several attempts have already been made at establishing a taxonomy for data localisation requirements, and many academics have considered both data localisation requirements and transfer limitation requirements as different categories of essentially the same type of regulation.¹⁰ Notably, Benjamin Wong further suggested that all such requirements can be understood through two questions – the “local processing” question (*ie*, what requirements are there on data controllers to process data within the territory of the country?), and the “transfer limitation” question (*ie*, to what extent is the data controller restricted from transferring a copy of the data out of the country?), respectively.¹¹

7 While there is merit in Wong's approach, a cross-jurisdictional snapshot with an alternative taxonomy separating data localisation from transfer limitation is provided in the table below. This table focuses specifically on *storage* requirements from the perspective of a potential transfer to a foreign jurisdiction, with the leftmost column being the most stringent (*ie*, data localisation) and the rightmost column being the most permissive (*ie*, transfer limitation).

10 Benjamin Wong, “Data Localization and the ASEAN Economic Community” (2020) 10(1) *Asian Journal of International Law* 158 at 164–165.

11 Benjamin Wong, “Data Localization and the ASEAN Economic Community” (2020) 10(1) *Asian Journal of International Law* 158 at 164–165.

Country	Transfers Not Allowed, Local Storage Only	Transfers Allowed, Local Copy Required	Transfers Allowed, No Local Copy Required
China	CIIOs: ✓ ¹²		non-CIIOs: ✓ ¹³
Europe (GDPR)			✓ ¹⁴
Hong Kong			✓ ¹⁵ (not in force)
India		Critical and sensitive personal data: ✓ ¹⁶ (not in force and subject to finalisation)	Non-critical and non-sensitive personal data (not in force and subject to finalisation)

-
- 12 Article 37 of China’s Cybersecurity Law (effective 1 June 2017) requires, *inter alia*, “personal information” and “important data” collected or produced by critical information infrastructure operators (hereinafter “CIIOs”) to be stored in China only. Other industry-specific requirements also apply to financial and medical institutions.
- 13 For non-CIIO network operators in China, security assessments will, depending on whether certain thresholds are crossed, need to be conducted either by the network operator or a competent Chinese regulator prior to any transfer.
- 14 Under the GDPR, transfers to countries outside the European Union and the European Economic Area are subject to certain requirements including, but not limited to, adequacy decisions by the European Commission, specific certifications, standard contractual clauses, binding corporate rules, or an applicable derogation such as consent or contractual necessity.
- 15 At the date of this article’s publication, s 33 of Hong Kong’s Personal Data (Privacy) Ordinance (Cap 486) relating to cross-border transfers has not come into force. However, a voluntary guidance on cross-border data transfers was published by Hong Kong’s Office of the Privacy Commissioner in December 2014.
- 16 Sections 33 and 34 of India’s Personal Data Protection Bill allow sensitive personal data to be transferred outside India but impose a requirement for such data to continue being stored in India. Critical personal data can only be processed in India and may only be transferred in two specific circumstances relating to health and emergency services or government permission.

Indonesia	Public operators: ✓ ¹⁷		Private operators: ✓ ¹⁸
Singapore			✓ ¹⁹
South Korea	Electronic medical and financial records: ✓ ²⁰		Other personal data: ✓
Vietnam		✓ ²¹	

8 From a legal or privacy practitioner's perspective, the distinction between data localisation requirements (*ie*, those which relate primarily to storage) and transfer limitation requirements are crucial, given the very different practical and commercial considerations required when coming up with an actual compliance solution. For example, while businesses can rely on organisational solutions such as binding corporate rules²² ("BCRs") or standard contractual clauses²³ to satisfy transfer limitation requirements, data localisation requirements require technically-focused solutions, such as

17 Under Government Regulation No 71 of 2019 on Electronic Systems and Transactions enacted in October 2019, "public electronic systems operators" are required to establish a local data centre. Private operators are able to locate their data and the electronic systems that hold them either in Indonesia or abroad.

18 Under Government Regulation No 71 of 2019 on Electronic Systems and Transactions enacted in October 2019, "public electronic systems operators" are required to establish a local data centre. Private operators are able to locate their data and the electronic systems that hold them either in Indonesia or abroad.

19 Section 26 of the Personal Data Protection Act 2012 (Act 26 of 2012) and reg 9 of the Personal Data Protection Regulations 2014 (S 362/2014) require certain requirements to be met prior to any transfer of personal data out of Singapore.

20 Under the relevant Korean regulations for the financial and medical sectors, certain types of financial and medical data may only be physically stored in Korea.

21 Under the Vietnamese Law on Cybersecurity which came into effect on 1 January 2019, certain types of user data (*eg*, those which are uploaded by users, or which relate to user relationships) must be stored within Vietnam for specific time periods based on their type.

22 GDPR Art 47.

23 GDPR Arts 28(6)–28(8).

sourcing for an appropriate local data centre, tracking users through unique technical identifiers (eg, IP address), and ensuring that the relevant network infrastructure is capable of distinguishing and storing the relevant datasets appropriately.

9 Data localisation requirements and transfer limitation requirements also affect data innovation in drastically different ways. In the next section, it is argued that transfer limitation requirements are better placed to enhance data protection, with less negative impact on innovation than data localisation requirements.

III. The impact of data localisation and transfer limitation on data innovation

10 Data localisation requirements, such as local storage and the creation of local copies, are justified through arguments which generally fall into four categories: (a) improved information security or cybersecurity; (b) greater individual privacy; (c) national security concerns; and (d) greater control and access for national regulators and law enforcement. While there is a considerable point to be made concerning in-country job creation (eg, in local data centres), such concerns are outside the scope of this article.

11 *Prima facie*, the goals of information security, *viz*, the confidentiality, integrity, accuracy and availability of data, may be served through data localisation requirements. Generally, data stored in a secure local data centre would be physically inaccessible by bad actors located abroad without any other means of access, technological or otherwise. Data integrity is also more likely to be preserved, as the risk of alteration or corruption from transit or transfer is reduced. In-country storage also ensures such data is accessible when needed.

12 In varying degrees, data localisation requirements also allow governments to address national security concerns more easily. National secrets, such as those which relate to the military, could be kept out of the jurisdictional reach of foreign governments which may rely on law enforcement or their own national security laws to seize the physical servers on which such data is stored.

13 However, this does not mean that data transferred and stored abroad is necessarily less secure. Local infrastructure may very well be less secure than foreign infrastructure, especially in countries where local data centres

are not as well-maintained or built on ageing physical assets. As noted by Han-Wei Liu in the context of foreign surveillance activities, “forcing firms to use local servers rather than those managed by their global counterparts, which are driven by fierce market competition to take more rigorous security measures to attract customers, data localization rules increase, rather than decrease, the risk of surveillance activities”.²⁴

14 More significantly, data localisation requirements run contrary to the concept of data innovation. As mentioned briefly above, the underlying technology infrastructure of many popular SaaS services (*eg*, customer relationship management platforms and human resources management platforms) are stored in servers located in developed jurisdictions, which organisations subject to a local storage requirement will not be able to utilise. As a result, cost savings which may arise out of such use are unavailable, forcing businesses to rely on inferior workarounds or more expensive alternatives. In the same vein, the ability of local companies to collaborate with foreign companies, such as for a commercial joint venture, will be severely curtailed if data that is crucial for the success of such a joint venture cannot even be transferred abroad.

15 A data subject's right to data portability may also be indirectly affected by localisation requirements, in the context where a receiving organisation is located abroad or has data stored in a data centre located abroad. The benefits that come with such a right (*eg*, broader consumer choice, continuity and preservation of past records) cannot be realised, as any porting request would constitute a cross-border data transfer unless the receiving organisation or its data centre is also located in-jurisdiction. In an age where mobile virtual network operators and digital banks are the norm rather than the exception, service providers will be faced with the choice to either duplicate storage infrastructure costs (*eg*, for local storage in each jurisdiction where it operates) or suffer business loss.

16 In comparison, compliance with transfer limitation requirements is far simpler – typically through standard contractual clauses or BCRs as mentioned above, or by ensuring that foreign law provides a standard of

24 Han-Wei Liu, “Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism” in *ASEAN Law in the New Regional Economic Order, Global Trends and Shifting Paradigms* (Pasha L Hsieh & Bryan Mercurio eds) (Cambridge University Press, 2019) at p 377.

protection that is at least comparable to that under local law.²⁵ By so doing, transfer limitation requirements achieve the same result as data localisation requirements; data confidentiality, integrity and accuracy can be maintained through obligations imposed by way of contract or by foreign law. On a practical level, data availability may even be augmented as authorised individuals receive faster response times from servers located nearer to them. Commercially, this translates to decreased compliance costs and more opportunities for global collaboration, while still respecting the need to protect personal data.

IV. Conclusion

17 As shown above, while data localisation requirements and transfer limitation requirements both serve to address the same underlying issues of privacy and information security, data innovation is better served through transfer limitation requirements. Overly strict data localisation requirements stifle innovation by making cost savings unavailable to customers, while also raising compliance costs for service providers. Further, the effectiveness of data localisation requirements depends on non-legal factors, such as in-country infrastructure quality. Conversely, transfer limitation requirements are able to achieve the exact same goals without stifling innovation in a digital economy and data-driven world.

25 Similarly, the European Commission is empowered under Art 45 of the GDPR to render adequacy decisions on the level of protection afforded by third countries.

THE EXPANDING ROLE OF THE RETENTION LIMITATION OBLIGATION IN THE MODERN DAY*

Jansen AW[†]

LLB (National University of Singapore);

Advocate and Solicitor (Singapore);

CIPP/E, CIPP/A, CIPM, FIP

Kenneth TAN[‡]

LLB (National University of Singapore);

Advocate and Solicitor (Singapore)

I. Retention limitations in the data economy

1 In an age of big data,¹ companies and organisations are increasingly recognising the value of the personal data collected from consumers in their normal course of business. The potential to turn aggregated data into monetisable assets for analytics, insights and ultimately new revenue streams cannot be understated. As early as 2011, a study commissioned by the World Economic Forum predicted that personal data would emerge as a new asset class touching on all aspects of society; a new resource as valuable as oil, with vast untapped wealth creation opportunities.² Almost

* 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, Donaldson & Burkinshaw LLP.

‡ Senior Associate, Donaldson & Burkinshaw LLP. Kenneth's main area of practice is in civil litigation with a particular focus on healthcare law and medico-legal issues.

1 Big data is popularly defined to mean "high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation": <<https://www.gartner.com/en/information-technology/glossary/big-data>> (accessed 4 February 2020).

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

a decade later, worldwide revenues for big data and business analytics solutions were projected to reach US\$189.1bn in 2019.³

2 When viewed through the prism of a potentially monetisable asset, it is understandable that organisations and especially for-profit entities may wish to retain personal data for purposes and durations beyond what was originally intended. What rules are in place to prevent the unbridled retention of, and profiteering from, consumer personal data?

3 One of the most direct restrictions would of course be that against retaining personal data in perpetuity. This is a feature of most current data protection regimes in one form or the other. For example, Art 17 of the European Union’s General Data Protection Regulation⁴ (“GDPR”), commonly analogised as a “right to be forgotten”, promulgates a robust set of criteria under which organisations are obliged to delete personal data including, particularly, when such data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.⁵ A more self-regulated approach can be seen in Canada. Paragraph 4.5.2, Schedule 1 of the Personal Information Protection and Electronic Documents Act⁶ (“PIPEDA”) requires companies to develop their own retention policies, including with respect to minimum and maximum retention periods. In doing so, organisations are advised to consider whether retaining personal information any longer would result in prejudice against the concerned individual or increase the risk of and exposure to potential data breaches.⁷

4 In Singapore, the Personal Data Protection Act 2012⁸ (“PDPA”) also imposes obligations on organisations pertaining to the retention of personal data, also known as the “Retention Limitation Obligation”. Under s 25 of the PDPA, organisations are to cease retaining documents containing personal data, or remove the means by which the personal data can be

3 International Data Corporation, “IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach \$189.1 Billion This Year with Double-Digit Annual Growth Through 2022” (4 April 2019).

4 (EU) 2016/679; entry into force 25 May 2018 (hereinafter “GDPR”).

5 GDPR Art 17(1)(a).

6 SC 2000, c 5.

7 Office of the Privacy Commissioner of Canada, “Personal Information Retention and Disposal: Principles and Best Practices” (June 2014) under the section “Retention Periods”.

8 Act 26 of 2012.

associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer served by retaining the data; and (b) retention is no longer necessary for legal or business purposes. It has been held that both limbs of s 25 are meant to be read disjunctively. Hence, an organisation is permitted to retain personal data if it can show that its retention purposes fall within either limb.⁹

5 Traditionally, the Retention Limitation Obligation is seen to play a neighbouring, albeit secondary, role to other data protection obligations. Generally, an organisation found to be in breach of the Retention Limitation Obligation is also likely to be in breach of its Protection,¹⁰ Accuracy¹¹ or Purpose Limitation Obligations.¹² This is also evident in the Personal Data Protection Commission's ("PDPC") *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*,¹³ which frames the issue of indeterminate retention periods in terms of increased risks of contravening other data protection provisions like the Protection Obligation.¹⁴ For example, one can envisage a situation where the unprincipled retention of personal data in perpetuity creates, in itself, a perpetual risk of unauthorised access or disclosure of the said data. As data accumulates over time by the perpetual retention, there is an increasing chance of a data breach to some or all of the data. Such breaches may have potential to be especially pronounced and severe in industries where collecting a large volume of detailed and sensitive personal data is necessary to fulfil business functions, eg, life insurers.¹⁵ The tendency, therefore, is to view the prolonged

9 *Re Social Metric Pte Ltd* [2018] PDP Digest 281 at [28].

10 *Re Social Metric Pte Ltd* [2018] PDP Digest 281; *Re O2 Advertising Pte Ltd* [2020] PDP Digest 398; *Re MSIG Insurance (Singapore) Pte Ltd* [2020] PDP Digest 495.

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

12 *Re Naturally Plus Singapore Pte Limited* [2017] PDP Digest 230.

13 Revised on 9 October 2019.

14 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) at para 18.2.

15 Indeed, insurance companies (particularly those offering personal lines), or their agents, have been the subject of a significant number of enforcement actions; see *Re AIA Singapore Private Limited* [2017] PDP Digest 73; *Re Aviva Ltd* [2017] PDP Digest 107; *Re Ang Rui Song* [2018] PDP Digest 236; *Re Aviva Ltd* [2018] PDP Digest 245; *Re Aviva Ltd* [2019] PDP Digest 145;

(continued on next page)

retention of personal data in terms of its potential to cause other harms, but not as a direct ill in itself.

6 However, as the digital economy transits to a new paradigm of data economy,¹⁶ new tensions will undoubtedly surface with respect to an individual's right to restrict the use of his personal data or even exploit it for his own benefit, *versus* the profit motives of organisations in possession of large datasets. While the contours of the big data landscape are constantly evolving, this article will posit three areas in which the Retention Limitation Obligation may be effective in enhancing the value of personal data (as a commodity) and rebalancing the scales towards greater empowerment of individual and consumer rights.

II. The Retention Limitation Obligation as a protector against prejudicial profiling from obsolete personal data

7 Modern organisations accumulate a significant amount of data on their stakeholders and customers. This can range from passively (and unconsciously) collected information from interactions with products or services such as location data or GPS co-ordinates from mobile phones (*ie*, user-activity), to information requiring active input such as residential addresses and credit card/bank account details to complete online transactions (*ie*, user-provided).

8 Repeated transactions and information transfers from the use of digital products or services may allow organisations to aggregate consumer/user data. This accumulated volume allows them to engage in profiling of individuals and groups of consumers/users, especially with the use of artificial intelligence ("AI") processes. The UK's Information

Re AIG Asia Pacific Insurance Pte Ltd [2019] PDP Digest 189; *Re NTUC Income Insurance Co-operative Ltd* [2019] PDP Digest 208; and *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 363.

16 Data economy has been defined as the measure of the overall impact of the data market, *ie*, "the marketplace where digital data is exchanged as products or services derived from raw data – on the economy as a whole": see European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – 'Building a European Data Economy'" (10 January 2017) at fn 1.

Commissioner's Office ("ICO") defines profiling as a form of data analytics in which aspects of an individual's personality, behaviour, interests and habits are analysed to make predictions or decisions about them.¹⁷ This includes the act of creating a profile, as well as automated decision-making using profiling.

9 In tandem with the growing ubiquity of big data analytics services, there is an increasing need to protect individuals against potentially adverse effects of profiling by organisations. It is certainly not doubted that there are innocuous and even arguably beneficial uses of profiling, such as enabling retailers to display targeted online advertisements based on one's search or social media activity. On the flip side, potentially abusive applications of profiling may prove intrusive or prejudicial, and may have significant social, economic or legal impact on the individual. Oftentimes (but not always), this arises when profiling is employed with automated decision-making.¹⁸ As an example, Recital 71 of the GDPR refers to scenarios where one is subject to an automatic refusal of an online credit card application or e-recruiting practices without any human intervention.¹⁹

10 Accordingly, some data protection regimes acknowledge the need to safeguard against negative outcomes of profiling. The GDPR forbids subjecting an individual to decisions based *solely* on automated processing, including profiling, if this would produce legal effects or significantly affect them, barring certain exceptions.²⁰ While Canada's PIPEDA does not contain such express restraints, the Office of the Privacy Commissioner of Canada cautioned that data analytics (including other types of profiling or categorisation) resulting in inferences being made about individuals or groups, which could lead to discrimination based on prohibited grounds

17 UK Information Commissioner's Office, "What is Automated Individual Decision-making and Profiling?" (5 June 2018) at p 6.

18 This refers to the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data – see UK Information Commissioner's Office, "What is Automated Individual Decision-making and Profiling?" (5 June 2018) at p 7.

19 GDPR Recital 71.

20 GDPR Art 22.

contrary to human rights law, will always fail the “appropriate purpose” test under s 5(3) of the PIPEDA.²¹

11 In Singapore, the concept and treatment of “data profiling” is taking its own unique shape in the form of “derived data” referred to in the PDPC’s discussion paper on data portability. Broadly speaking, derived data refers to new data created through the processing of other data by applying business-specific logic rules,²² with the objective of deriving new business insights from consumers’ user-provided and user-activity datasets, which in turn unlocks new commercial value and consumer benefits.²³ This definition of “derived data” is both an enlightened and useful one – it seeks to take the good from what can be derived from data profiling of individuals, such as being able to customise the service for the individual, while leaving behind the bad or the negatives from the traditional norms of data profiling, such as stigma or discrimination relating to individuals. While this concept has yet to be put to the test, it looks to be promising for the future.

12 Given the potentially wide-ranging impact that data profiling (especially automated decision-making) can have on daily life, it is imperative that individuals are protected from the prejudicial application of outdated or obsolete personal data, especially since an individual’s circumstances do not remain static. Multiple irrelevant online advertisements arising from one’s surfing habits in the past year may be a mild annoyance at worst. Outdated financial history resulting in one being denied essential banking facilities would be, on the other hand, clearly more significant. In such situations, the protective function of the Retention Limitation Obligation becomes readily apparent, especially when

21 Office of the Privacy Commissioner of Canada, “Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)” (May 2018) under the section “Inappropriate Purposes or No-Go Zones”.

22 See Personal Data Protection Commission, “Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions” (22 May 2019) at paras 3.12–3.13. “Processing” has also been defined as including “the use of any mathematical, logical, statistical, computational, algorithmic, or analytical methods” (see para 2.28, fn 13).

23 See Personal Data Protection Commission, in collaboration with the Competition and Consumer Commission of Singapore, “Discussion Paper on Data Portability” (25 February 2019) at paras 3.4 and 3.22.

employed in tandem with other existing safeguards such as the Accuracy or Correction Obligations to preserve the accuracy of datasets.

13 However, this only addresses the currency of the data that was obtained from the individual (“input personal data”). There can equally be issues of the derived data itself being outdated. In such circumstances where the derived data, which has already been delinked from the input personal data, is outdated, this may lead to wrong decisions; and without the original input personal data, it may be difficult to rectify the profile or model. The solution may lie in retaining the input personal data but perhaps in an anonymised form to preserve the utility of the dataset without expunging it wholesale.²⁴ As the saying goes: one should not use a sledgehammer to crack a nut. In this regard, the Retention Limitation Obligation, which sometimes acts like an overly blunt tool in mandating the deletion and destruction of personal data, may not be the solution in all such cases.

14 On a more quotidian level, one may consider the PDPC's decision in *Re Credit Bureau (Singapore) Pte Ltd*²⁵ (“*Re Credit Bureau*”). Although that case did not involve the application of leading-edge data profiling technologies, it underscores the potential prejudice that may result from the collection, use and disclosure of outdated personal data for, *inter alia*, commercial purposes.

15 In *Re Credit Bureau*, a credit bureau had displayed bankruptcy information including a “HX” risk grading in its Enhanced Consumer Credit Report (“ECCR”) of the complainant. The organisation explained that a “HX” risk grade meant that there could be a past or existing bankruptcy record associated with the individual in question but did not determine creditworthiness. The complainant had a previous bankruptcy application filed against him which was withdrawn a month later.

16 The organisation rejected the complainant's request to amend his risk grading, informing him that it was the organisation's practice to display bankruptcy-related data for five years. Dissatisfied, he complained to the

24 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) at paras 18.10 and 18.14.

25 [2019] PDP Digest 227.

PDPC that the organisation had retained his personal data when it was no longer necessary for legal or business purposes.

17 The PDPC found that the organisation did not breach s 25 of the PDPA as its display period of five years for bankruptcy-related information in the ECCR aligns with the display period of the publicly available insolvency search maintained by the Insolvency and Public Trustee Office (“IPTO”) and was therefore not unreasonable. More pertinently, the PDPC also recognised the nature of the organisation’s business, namely that it provides credit reporting services, and hence concluded that the retention of bankruptcy-related information in order to deliver its services was a valid business purpose.

18 As can be seen, the organisation succeeded in establishing the “business purpose” limb of s 25 because of the association between its five-year retention period and the retention period of an analogous service offered by a government department. At first blush, this begs the question of whether a different result would have transpired if the organisation’s retention period had been longer.

19 More pertinent to the discussion, however, the facts in *Re Credit Bureau* may be regarded as a harbinger of the kinds of unwelcome effects individuals may face when their personal data constitutes the stock-in-trade for businesses offering information services. Such concerns are only likely to be exacerbated with the rapid expansion of more sophisticated types of analytics services dealing with wider-ranging categories of personal datasets.

20 It is therefore envisaged that the Retention Limitation Obligation will play a greater role in the modern use of data analytics, profiling and derived data that will be inseparable features of the data economy.

III. The Retention Limitation Obligation as an enabler for the commercialisation of personal data

21 Thus far, the discussion around the use of personal data has largely centred around the imperatives of organisations. This is unsurprising since the collection, use and disclosure of personal data is still largely geared towards fulfilling business functions or enhancing commercial growth and

value in business models.²⁶ Generally speaking, it is expected that individuals and consumers will lack the technical wherewithal, expertise or capacity to exploit such datasets for revenue generating functions. However, it is postulated that increasing sophistication of big data technologies, including the widespread adoption of AI and machine learning (or other technical mechanisms) in many sectors, will unlock new means for individuals to commercialise their personal data.

22 While this article is not intended as a primer on AI, some introductory remarks on its key features and how it relates to the use of data would be timely. In this regard, the authors adopt the concise model describing the AI deployment process in the PDPC's discussion paper.²⁷

23 The first stage of the AI deployment process involves data preparation, whereby raw data is formatted and cleansed so that conclusions can be drawn accurately. It is generally understood that accuracy and usefulness of insights derived down the line increase with the relevance and amount of data gathered at this stage.

24 In the second stage, algorithms are applied for analysis. This includes statistical models, decision trees and neural networks. This part of the process is commonly known as machine learning, which may be defined as the set of techniques and tools that allow computers to "think" by creating mathematical algorithms based on accumulated data.²⁸ Machine learning can be differentiated into "supervised" and "unsupervised".²⁹ In supervised

26 See Niko Mohr & Holger Hürtgen, "Achieving Business Impact with Data: A Comprehensive Perspective on the Insights Value Chain" *Digital McKinsey* (April 2018); and Josh Gottlieb & Khaled Rifai, "Fueling Growth Through Data Monetization" *McKinsey & Company* (December 2017).

27 Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI" (5 June 2018) at p 4.

28 UK Information Commissioner's Office, "Big Data, Artificial Intelligence, Machine Learning and Data Protection" (4 September 2017) at pp 7–8.

29 Some authors recognise additional or hybrid types/techniques of machine learning algorithms, *eg*, semi-supervised, reinforcement, deep, ensemble, *etc* – see, *eg*, Hunter Heidenreich, "What Are the Types of Machine Learning?" *Towards Data Science* (5 December 2018); and Nicolaus Henke *et al*, "The Age of Analytics: Competing in a Data-Driven World" *McKinsey Global Institute* (December 2016) at pp 23–24.

learning, algorithms are developed or “trained” based on labelled datasets/outputs and therefore create models of the world on which predictions can then be made.³⁰ In unsupervised learning, algorithms are not trained based on labelled outputs. Instead, they are left to infer the natural structure present within a set of data points.³¹ The results and algorithms are reiterated until a model that produces the most useful results emerges.

25 In the third stage, a chosen model is used to produce probability scores with a variety of applications. These include delivering insights, determining relationships and making predictions about trends.

26 Perusing the above, the individual whose data is collected can surely be regarded as an equally valid participant and stakeholder in the development process, namely at the crucial data preparation, or collection, stage. This perspective is often overlooked as the AI value chain normally focuses on developers, user companies and consumers/clients of those companies.³² Furthermore, individuals and consumers tend to be associated with the products, or targets, of AI applications³³ (*ie*, the “output” stage) and are not regarded as key drivers of the value chain.

27 Bearing this in mind, it is not impossible to envisage that the broadening applications of sophisticated AI processes in more sectors and industries would drive up the value of data (including personal data). Where data has hitherto been collected for specific, discrete or one-off uses, it is now employed to unlock and create economic value and innovation by combining datasets through varied, multiple uses.³⁴ At some point, both

30 UK Information Commissioner’s Office, “Big Data, Artificial Intelligence, Machine Learning and Data Protection” (4 September 2017) at pp 7–8.

31 Devin Soni, “Supervised vs. Unsupervised Learning” *Towards Data Science* (22 March 2018).

32 Personal Data Protection Commission, “Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI” (5 June 2018) at p 3.

33 See, *eg*, Patrick Hall *et al*, “The Evolution of Analytics: Opportunities and Challenges for Machine Learning in Business” *SAS* (May 2016) at pp 4–6; and Nicolaus Henke *et al*, “The Age of Analytics: Competing in a Data-Driven World” *McKinsey Global Institute* (December 2016) at pp 29–34.

34 World Economic Forum, “Unlocking the Value of Personal Data: From Collection to Usage” (February 2013).

individuals and businesses may begin to put a price on data as a tradeable commodity in itself. Indeed, the sale of consumer data has been widespread among commercial entities, including “data brokers” involved in buying, collecting and selling personal information, prompting some jurisdictions to enact regulatory safeguards requiring mandatory registration of businesses engaged in this trade.³⁵

28 A defining feature of data, when contrasted with other commodities, is that it appears to be infinitely usable and does not diminish with simultaneous use, which further strengthens the business case for its widespread monetisation.³⁶ Data as a property right is far from a radical idea, even though this conceptualisation is still largely in its nascent form. In daily life, consumers already implicitly recognise the notion of trading their privacy (by sharing personal information) to businesses in return for personalised products, services and offers; this risk-benefit trade-off has been termed the “give-to-get” ratio.³⁷ Taking the idea of data monetisation one step further, California Governor Gavin Newsom has openly talked of developing proposals for a “data dividend”, under which the staggering value³⁸ generated from technology companies’ use of collected personal data is returned to the public in some form (*eg*, via tax revenues, or refunds to consumers).³⁹ A contender for the 2020 US Presidential elections had also advocated expanding the bundle of individual and proprietary rights associated with data.⁴⁰

35 Steve Melendez & Alex Pasternack, “Here Are the Data Brokers Quietly Buying and Selling Your Personal Information” *Fast Company* (3 February 2019).

36 Christopher Tonetti & Cameron F Kerry, “Should Consumers Be Able to Sell Their Own Personal Data?” *The Wall Street Journal* (13 October 2019).

37 Manish Bahl, “The Business Value of Trust” *Cognizant Centre for the Future of Work* (May 2016).

38 In 2019, Axios estimated that the value of the average monthly active user is worth US\$7.37 to Facebook and US\$2.83 to Twitter – see Sara Fischer, “Reddit’s Exponential Value Rise” *Axios* (12 February 2019).

39 Don Thompson, “California Governor Wants Users to Profit from Online Data” *The Associated Press* (14 February 2019).

40 Andrew Yang, “Data as a Property Right” *Yang 2020* <<https://www.yang2020.com/policies/data-property-right/>> (accessed 4 February 2020).

29 Following this train of thought, it is possible to envisage the further development of a market for trade in the temporary (exclusive or non-exclusive) rights to possess, use and disclose personal data. While most individuals would likely balk at the notion of putting up for sale personal information to be held absolutely and in perpetuity by a purchaser (usually an organisation), this becomes more palatable if defined time limits are put on the purchaser's right to access that data, normally by way of contractual agreement. Data as a limited proprietary right may well become a distinct and viable asset class. After all, AI developers require datasets to train algorithms, but may have no further use for it once suitable models have been derived following the reiterative machine learning process.

30 In such a scenario, an expanded conceptualisation of the Retention Limitation Obligation might play a key role in enabling individuals to unlock the value in their personal data. An additional statutory carve-out could be devised to facilitate an individual's sale of personal data to organisations for defined time periods, with cessation of retention in accordance with contractual terms.

31 The interplay between contractual rights, the withdrawal of consent under the PDPA, and the Retention Limitation Obligation becomes important here. A contract that stipulates the retention of personal data for a defined time period is akin to a withdrawal of consent under the PDPA at that defined time. Under the PDPA, the withdrawal of consent tends to come hand in hand with the Retention Limitation Obligation, in that if an individual withdraws his consent to the continued use or disclosure of personal data, it is often that the organisation has no further purposes (legal, business or otherwise) to retain the data under the Retention Limitation Obligation. Nevertheless, given that the purposes under the Retention Limitation Obligation refer to those of the organisation as opposed to the individual (*ie*, the organisation's legal purpose), there is always a chance that the organisation may be allowed to retain the data for its legitimate purposes notwithstanding that the individual has withdrawn consent and/or the contract provides for its destruction. Thus, for this proposed business model to work, the Retention Limitation Obligation would need to be aligned with the contract and the withdrawal of consent of the individual to cease all retention of personal data.

32 There is also another dynamic between the withdrawal of consent and contractual rights at play here. If the individual has agreed that his personal

data can be used for x years in exchange for the benefits of participating in this scheme, would that effectively limit his ability to withdraw consent before x years is up? Conversely, if the individual withdraws his consent early, does it allow him to extricate himself from the contract terms of allowing the organisation to retain the personal data for x years? One solution is for contractual rights to generally take precedence over statutory rights under this proposed business model in enabling the commercialisation of data. That being said, there may still be a need for some statutory safeguards to protect vulnerable individuals from unscrupulous organisations. In this regard, there is scope for the PDPA to play a role in shepherding the principled development of data commercialisation contracts.

33 Naturally, the existing safeguards under the PDPA, including the purpose-centric criteria under the Retention Limitation Obligation, should be preserved by default for individuals who choose not to participate in this market.

IV. The Retention Limitation Obligation as an enabler for altruistic data sharing

34 Aside from raw revenue generation, a data trading economy may unlock additional non-monetary value by enabling better delivery of public sector services such as in healthcare, education and transport. In its 2017 report, the UK's ICO cited examples of big data analytics being used for social good, such as in implementing initiatives to increase cancer diagnosis rates, identifying trends to improve higher education processes, and revealing travel patterns across rail and bus networks to benefit travellers in London.⁴¹ A case study in Abu Dhabi has shown that undertaking personalised individual interventions by leveraging public health data can lead to improvement in outcomes for chronic diseases.⁴² In the words of a data-sharing proponent, “[e]very hospital cannot use the world’s most

41 UK Information Commissioner's Office, “Big Data, Artificial Intelligence, Machine Learning and Data Protection” (4 September 2017) at pp 15–17.

42 World Economic Forum, “Unlocking the Value of Personal Data: From Collection to Usage” (February 2013) at pp 9 and 26.

talented surgeon simultaneously, but they can all potentially employ the best data”.⁴³

35 While the potential social benefit of big data analytics is readily apparent, a limiting factor would be the inability of public institutions or non-governmental organisations (“NGOs”) to access such datasets, especially when social good is subordinated to profit imperatives in the context of a data trading economy. In such an economy driven by profits and the value of personal data, there is, it is contended, a greater incentive for companies to hoard personal data and preserve its value by limiting access to such data to obtain a competitive advantage. Concomitantly, the commercial machinery will incentivise individuals to put their personal data with the companies that can afford to purchase it, thereby leaving out those that can ill afford it. This may lead to a downward trend of altruistic data sharing.

36 In such a scenario, the Retention Limitation Obligation can conceivably facilitate a data-sharing ecosystem, thus allowing non-profit entities to overcome resource hurdles. Ideally, the Retention Limitation Obligation will be paired with legislation empowering public (and suitably-assessed non-profit) entities to collect and aggregate specific categories of personal data for specific applications relevant to discharging their social function. This may also be achieved by expanding the PDPA’s existing categories of exceptions to consent for public agencies to include the use and disclosure of personal data by public and non-profit entities undertaking activities for social good (and not for commercial enterprise). In any event, an opt-out should be provided to preserve the individual agency of those who choose not to participate in altruistic data sharing.⁴⁴

37 The existing purpose-centric test under the Retention Limitation Obligation would therefore be useful in setting the limits of defined termination events (*eg*, the conclusion of a specific data analytics project)

43 Christopher Tonetti & Cameron F Kerry, “Should Consumers Be Able to Sell Their Own Personal Data?” *The Wall Street Journal* (13 October 2019).

44 An analogous example of an enforced social good with an opt-out feature is Singapore’s Human Organ Transplant Act (Cap 131A, 2012 Rev Ed), which was enacted to allow, *inter alia*, organ removal and recovery from deceased Singaporeans and permanent residents for transplantation to other living persons unless they have opted out.

upon which the disposal or anonymisation of personal data will be mandatory. In fact, anonymisation may be the preferred way of striking the appropriate balance between allowing organisations to continue deriving use from datasets, while at the same time guaranteeing individual privacy rights. This accords with current guidelines recognising instances where anonymised data may be used where personal identifiers are unnecessary or undesired.⁴⁵ With such mechanisms in place, the wider public may thus be incentivised to participate actively in such altruistic data sharing which could in turn bring large-scale social benefits, while also being assured that their personal data would not remain held by organisations in perpetuity which carries with it the attendant risk of data breaches.

V. Concluding thoughts

38 It remains to be seen whether the role of the Retention Limitation Obligation will expand in the manner described in this article. What is clear, however, is that large-scale commercialisation of data is already a reality, and big data analytics will continue to drive expansion and create value in all sectors of the economy. It is therefore timely to relook at the Retention Limitation Obligation and explore ways it may be modified to cater to modern-day uses. The notion of placing defined time limits on the retention of data will always remain a crucial safeguard against the excesses of privacy intrusions, and in minimising the risk of other data harms. As discussed above, the existing purpose-centric nature of the Retention Limitation Obligation does to a degree address the challenges of postulated data commercialisation models. It is hoped that with further development, the Retention Limitation Obligation can become a vital pillar to enable realisation of personal data's value (in all its new and emerging forms) for the benefit of individuals and consumers.

45 See Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 3.5.

PREVENTING AND MANAGING DATA INCIDENTS: LESSONS FROM THE PERSONAL DATA PROTECTION COMMISSION'S ENFORCEMENT DECISIONS*

LIM Chong Kin[†]

LLB (Hons) (National University of Singapore),

LLM (National University of Singapore);

Advocate and Solicitor (Singapore); Solicitor (England & Wales)

Janice LEE[‡]

LLB (Hons) Law with Chinese Law (University of Nottingham);

Advocate and Solicitor (Singapore); CIPP/E; CIPM

I. Introduction

1 Since the Personal Data Protection Act 2012¹ (“PDPA”) came into effect on 2 July 2014, the Personal Data Protection Commission (“PDPC”)

* 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; Managing Director, Corporate & Finance; Co-Head, Drew Data Protection & Cybersecurity Academy; Co-Head, Data Protection, Privacy & Cybersecurity Practice; Head, Technology, Media & Telecommunications Practice Group; Head, Competition, Consumer & Regulatory 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*.

‡ Associate Director, Data Protection, Privacy & Cyber-security Practice Group; Technology, Media & Telecommunications Practice Group, Drew & Napier LLC. Janice is a Certified Information Privacy Professional (Europe) (CIPP/E) and a Certified Information Privacy Manager (CIPM).

1 Act 26 of 2012.

has issued over 100 reported decisions (including summary decisions) and meted out financial penalties that amount to over \$2m.²

2 In 2019 alone, the PDPC issued a total of 51 enforcement decisions – the most since 2016 when the PDPC first started publishing its decisions. There was also an increase in the total quantum of financial penalties meted out by the PDPC in 2019; a total of 42 organisations were subject to fines ranging from \$1,000 to \$750,000. In contrast, the PDPC imposed financial penalties on only 13 organisations in 2018.

3 2019 was also a significant year for data protection in Singapore as it saw the introduction of a number of initiatives that marked the shift from compliance to accountability which began back in 2017. Apart from the launch of the Data Protection Trustmark certification system to recognise organisations with accountable practices, the PDPC's *Guide to Accountability under the Personal Data Protection Act*³ formally introduced the concept of accountability in relation to personal data protection and updated what was previously known as the Openness Obligation (ss 11 and 12 of the PDPA) to the Accountability Obligation. The coming amendments to the PDPA, which are expected to introduce an enhanced consent regime and mandatory data breach notification, are also set to further accentuate and integrate accountability within the PDPA.

4 As Singapore enters into the sixth year since the PDPA came into force, this article reflects on the substantial body of reported decisions and highlights the trends, recurring themes and lessons that may be discerned.

II. Overview of common causes of data incidents

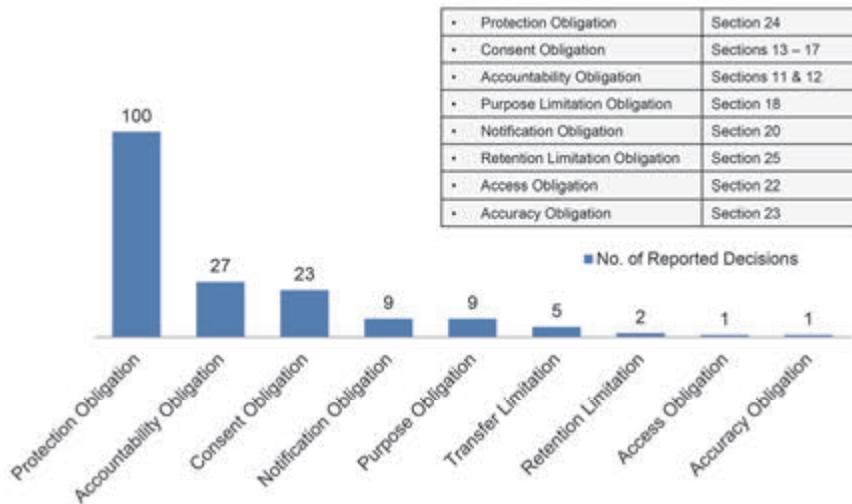
5 As with previous years, breaches of s 24 of the PDPA (the Protection Obligation) continue to feature strongly and constitute the overwhelming majority of the enforcement decisions issued by the PDPC. As of 20 April 2020, there have been 100 cases (approximately 72% of all published

2 As at 20 April 2020, a total of 138 decisions have been reported, and the combined amount of financial penalties amount to \$2,170,000.

3 Published 15 July 2019.

enforcement decisions) that dealt with the Protection Obligation.⁴ This is followed by cases concerning the Accountability Obligation and/or Consent Obligation.

Data Protection Enforcement – Reported Decisions (as at 20 April 2020)



6 Most of the data breach incidents can also be attributed to one of the several causes examined below.

A. Human error

7 First, it is clear from the cases that one of the most common causes of data incidents in Singapore is human error. This refers to the unauthorised disclosure of personal data due to mistakes generally made by employees within the organisation, particularly when an employee is tasked to send out correspondence (eg, hard-copy letters or e-mails) containing personal data to third parties. For example, in *Re SAFRA National Service Association*⁵ (“*SAFRA National Service Association*”), an employee of the organisation

4 Other common contraventions of the Personal Data Protection Act 2012 (Act 26 of 2012) include the Accountability Obligation (formerly known as the Openness Obligation) which featured in 25 decisions; and the Consent Obligation which featured in 23 decisions.

5 [2020] PDP Digest 511.

wrongly sent out two separate batches of e-mails attaching an Excel spreadsheet containing the personal data of certain members of the organisation's shooting club to other members.

8 There have also been a number of cases where employees misplaced or improperly disposed of data storage devices (eg, thumb drives) or other items containing personal data. For example, in *Re The Travel Corporation (2011) Pte Ltd*⁶ (“*The Travel Corporation*”), an employee of the organisation misplaced her laptop and portable hard disk which contained unencrypted files with the personal data of the organisation's customers, employees and suppliers on her way home.

9 Under s 53(1) of the PDPA, the actions of an employee are attributed to his employer.⁷ As such, organisations are generally liable for the data incidents even if the unauthorised disclosure was caused by a mistake made by its employee(s).

10 In this regard, the PDPC has said 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”.⁸ This is especially the case where the organisation does not have adequate data protection policies and procedures, such as data protection training for employees⁹ and/or a well-documented written data protection policy with specific practical guidance on handling personal data in the course of their employment,¹⁰ to protect against such risks. Such internal policies should be effectively implemented by operational frameworks and procedures.¹¹

6 [2020] PDP Digest 489.

7 Under s 53(1) of the Personal Data Protection Act 2012 (Act 26 of 2012), any act done, or conduct engaged in, by an employee in the course of employment shall be treated for the purposes of the Act as acts done, or conduct engaged in, by his employer as well as him.

8 *Re Aviva Ltd* [2018] PDP Digest 245 at [28]; *Re Furnituremart.sg* [2018] PDP Digest 175 at [21].

9 *Re Hazel Florist & Gifts Pte Ltd* [2018] PDP Digest 199 at [13]–[14].

10 *Re Aviva Ltd* [2018] PDP Digest 245; *Re SAFRA National Service Association* [2020] PDP Digest 511.

11 *Re The Travel Corporation (2011) Pte Ltd* [2020] PDP Digest 489.

11 In *Re Aviva Ltd*,¹² the organisation had a high-level data protection policy which listed out the nine data protection obligations and some basic “dos and don’ts”. This was found to be inadequate as an administrative security measure because it did not provide sufficient instructions or practical guidance for the processing staff concerning their specific duties.¹³

12 More recently, in *SAFRA National Service Association*, the PDPC reiterated that verbal instructions alone are insufficient as employees will not be able to refer to them in the course of their duties and may not be able to recall such instructions after some time. The PDPC also advised that the organisation should have a properly documented process for regular or frequent tasks such as sending out mass e-mails to members to publicise coming events.¹⁴

13 Another decision to be noted is *The Travel Corporation* where the organisation was found to be in breach of the Protection Obligation.¹⁵ Although the organisation had internal policies for portable storage devices, employees were only verbally instructed to not bring any portable storage devices out of the office. There were no operational frameworks or procedures to implement this policy in its individual business units. The organisation also did not implement any password protection policies or data encryption policies for its portable storage devices.

14 Where employees are required to carry out routine tasks manually with respect to sensitive personal data (eg, enveloping insurance policy documents), and there is a foreseeable risk that there may be inadvertent disclosure through human error, the PDPC recommends that the organisation implement additional monitoring or verification measures to minimise the risk of accidental mistakes.¹⁶ Such measures may include

12 [2018] PDP Digest 245.

13 *Re Aviva Ltd* [2018] PDP Digest 245 at [31]–[34].

14 *Re SAFRA National Service Association* [2020] PDP Digest 511 at [11].

15 *Re The Travel Corporation* (2011) Pte Ltd [2020] PDP Digest 489 at [7].

16 *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [30]–[33]. The Personal Data Protection Commission noted that the organisation did not have any arrangement or process to verify the accuracy of contact information or monitor the number of renewal notices it received by fax to contain any unauthorised disclosure.

second-layer or randomised checks to ensure that the tasks are performed correctly.¹⁷

15 For such regular and frequent tasks, the PDPC also recommends that organisations consider process automation tools (eg, mail-merge for monthly e-mail blasts) to minimise human error, but such systems and processes should be checked regularly to ensure their accuracy and reliability.¹⁸

B. Technical errors

16 Second, the authors note that the inadvertent unauthorised access or disclosure of personal data in a number of cases was caused by errors or bugs in the programming code of websites, databases and other software. For example, in *Re Friends Provident International Limited*,¹⁹ unauthorised third parties were able to access the personal data of policyholders due to a faulty JavaScript in the organisation's online portal.

17 Another common occurrence is when organisations unwittingly store personal data that they collect on online databases or in folders that are accessible by the public (eg, in *Re Tutor City*²⁰ and *Re Society of Tourist Guides Singapore*²¹).

18 In evaluating the organisations' security measures (or lack thereof), the PDPC has clarified what it considers to be reasonable security arrangements. These include:

- (a) Organisations should properly scope and devise tests to address the risks of unauthorised access or disclosure of personal data, and such tests should have in mind the intended design and functionality of the software or system.²²
- (b) Organisations should conduct vulnerability scans and penetration tests (where appropriate), in addition to standard

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

18 *Re SAFRA National Service Association* [2020] PDP Digest 511 at [9]–[10].

19 [2020] PDP Digest 377.

20 [2020] PDP Digest 170.

21 [2020] PDP Digest 531.

22 *Re Friends Provident International Limited* [2020] PDP Digest 377 at [9]; *Re i-vic International Pte Ltd* [2020] PDP Digest 485 at [11].

functional tests, to detect vulnerabilities.²³ A vulnerability scan or assessment is performed on the organisation's IT systems or network to identify flaws that may be exploited during an attack.²⁴ It is a "non-intrusive approach that serves to produce a prioritised list of security vulnerabilities".²⁵ In contrast, penetration testing uses an intrusive approach to discover security weaknesses in the organisation's IT infrastructure and applications by emulating a real attack to gain privileged access.²⁶ While these assessments serve different purposes, generally, periodic penetration testing would be required in cases where the IT systems and infrastructure are complex and/or the organisation is in possession or control of personal data that is sensitive in nature.²⁷

(c) Where the functionality of the system or software allows authorised individuals to access personal data through an identifier, organisations should be aware of the risk of manipulation of such identifiers and implement a second layer of authorisation or verification to obtain access to the personal data.²⁸

(d) Organisations should implement access controls to prevent personal data from being accessed by unauthorised users or indexed by web crawlers either by placing personal data in a non-public

23 *Re InfoCorp Technologies Pte Ltd* [2020] PDP Digest 282 at [12].

24 GOsafeonline, Cyber Security Agency of Singapore, "Vulnerability Assessment and Penetration Testing" (18 March 2014).

25 GOsafeonline, Cyber Security Agency of Singapore, "Vulnerability Assessment and Penetration Testing" (18 March 2014).

26 GOsafeonline, Cyber Security Agency of Singapore, "Vulnerability Assessment and Penetration Testing" (18 March 2014).

27 See, *eg*, *Re Genki Sushi Singapore Pte Ltd* [2020] PDP Digest 347 at [15(b)] and [19], where the Personal Data Protection Commission found that the failure to conduct periodic penetration tests was a significant gap in the security measures implemented in relation to the server containing sensitive personal data of its employees (*eg*, NRIC and passport numbers and bank account details).

28 *Re Friends Provident International Limited* [2020] PDP Digest 377 at [8]; *Re Ninja Logistics Pte Ltd* [2020] PDP Digest 473 at [10]; *Re InfoCorp Technologies Pte Ltd* [2020] PDP Digest 282 at [13].

folder/directory, or by instituting access restrictions within the sub-folder.²⁹

C. *Malicious activity*

19 Third, there have also been a number of recent cases where hackers or other malicious actors exploited existing vulnerabilities arising from a failure to implement basic technical security measures such as regular security testing and patching. This can range from attacks perpetrated by skilled and sophisticated threat actors (eg, *Re Singapore Health Services Pte Ltd*³⁰) to the more common brute-force attacks, e-mail phishing scams or ransomware attacks (eg, *Re Marshall Cavendish Education Pte Ltd*³¹).

20 From these cases, the authors observe and set out below a non-exhaustive list of technical security measures that an organisation should carry out to meet its Protection Obligation:

- (a) Regular patching should be carried out to protect the system against external threats, and the failure to do so may amount to a breach.³²
- (b) Technical measures such as firewalls should be configured carefully. Any lapses may expose the server to security risks and amount to a breach.³³
- (c) Strong passwords should be used for administrator accounts and should be strictly enforced.³⁴ Administrator accounts should also be properly managed by disabling unused or dormant accounts and deleting records.³⁵ The sharing of administrator accounts should be avoided and employee access to such accounts should be monitored.³⁶

29 *Re Tutor City* [2020] PDP Digest 170 at [21].

30 [2019] PDP Digest 376.

31 [2020] PDP Digest 425.

32 *Re Genki Sushi Singapore Pte Ltd* [2020] PDP Digest 347 at [20]–[21].

33 *Re Marshall Cavendish Education Pte Ltd* [2020] PDP Digest 425 at [18]–[24].

34 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [112]–[113].

35 *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133 at [50]; *Re K Box Entertainment Group Pte Ltd* [2017] PDP Digest 1 at [26].

36 *Re MSIG Insurance (Singapore)* [2020] PDP Digest 495 at [18(b)] and [18(d)]; *Re Spize Concepts Pte Ltd* [2020] PDP Digest 311 at [16].

21 Apart from the findings made in its reported decisions, the PDPC has also issued detailed and extensive guides on specific topics, including the *Guide to Securing Personal Data in Electronic Medium*,³⁷ the *Guide on Building Websites for SMEs*,³⁸ the *Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data*³⁹ and the *Guide to Printing Processes for Organisations*.⁴⁰

III. The Personal Data Protection Commission's enforcement of the Personal Data Protection Act 2012: Evolving expectations and key takeaways

22 As Singapore's data protection regime matures and the nature of the data breach incidents evolves, the PDPC's approach towards the data protection obligations and its expectations of what organisations are required to do to discharge their obligations under the PDPA has similarly evolved. This is not unexpected as a standard of reasonableness underpins the PDPA.⁴¹ In meeting their responsibilities under the PDPA, organisations are expected to have regard to what a reasonable person would consider appropriate in the circumstances. The standard of reasonableness is expected to be evolutionary and what is reasonable is not a black-and-white issue.⁴²

23 This section highlights how the PDPC's expectations of what organisations are required to do to discharge their obligations have developed over the years in three notable areas.

37 Revised 20 January 2017.

38 Revised 10 July 2018.

39 Issued 20 January 2017.

40 Issued 3 May 2018.

41 Section 11(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) provides that in meeting its responsibility under the Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

42 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) at para 9.5.

A. Reasonable security arrangements – Lack of technical expertise no excuse for failure to comply with the Personal Data Protection Act 2012

24 Section 4(3) of the PDPA states that an organisation has the same obligations 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. However, many organisations have sought to argue that they should not be liable for the failure to prevent the unauthorised disclosure of the personal data because they do not have the technical expertise and/or they outsourced the maintenance of their IT functions and security to an external IT services provider.

25 While the PDPC has always recognised that there may be different responsibilities that an organisation or data intermediary may undertake under the PDPA,⁴³ the PDPC has expressly stated in its recent cases that the responsibilities of ownership *do not* require technical expertise. The lack of technical expertise is no excuse or defence against the failure to take sufficient steps to comply with the PDPA.⁴⁴ Even if organisations delegate work to their contractors who are their data intermediaries, organisations as data controllers must ultimately take responsibility for the personal data processed on their behalf.⁴⁵

26 This position is encapsulated in the frequently cited passage from *Re WTS Automotive Services Pte Ltd*⁴⁶ where it said:

27 Further, organisations should take note that while they may delegate work to vendors to comply with the PDPA, the organisations' responsibility

43 Organisations which engage a third party to process personal data on their behalf are required to play a supervisory or general role for the protection of the personal data whereas the data intermediary will have a more direct or specific role in the protection of personal data.

44 See *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [27]–[28]; *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [54]–[56]; *Re DS Human Resource Pte Ltd* [2020] PDP Digest 274 at [15]; *Re Spize Concepts Pte Ltd* [2020] PDP Digest 311 at [6]; *Re Advance Home Tutors* [2020] PDP Digest 438 at [18]; *Re Zero1 Pte Ltd* [2020] PDP Digest 458 at [13]; *Re National Healthcare Group Pte Ltd* [2020] PDP Digest 517 at [17]; *Re Society of Tourist Guides (Singapore)* [2020] PDP Digest 531 at [13]; and *Re SCAL Academy Pte Ltd* [2020] SGPDPDC 2 at [9].

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

46 [2019] PDP Digest 317 at [27] and [28].

for complying with statutory obligations under the PDPA may not be delegated. In this case, the Organisation simply did not put in place any security arrangements to ensure that it complies with its obligations under s 24 of the PDPA.

28 The final point made by the Organisation in its representations is that it had no technical expertise to identify technical flaws and had no reason to suspect that the compromised URL links would be published on the Internet. In the present case, the gravamen lies in the lack of awareness and initiative on the part of the Organisation, as owner of the system, to take its obligations and responsibilities under the PDPA seriously. *It is unrealistic to expect all organisations to have the requisite level of technical expertise to manage increasingly complex IT systems. But a responsible organisation would have made genuine attempts to engage competent service providers and give proper instructions.* In this case, it is *the paucity of evidence of such instructions, purportedly made by the Organisation, that stands out. Likewise, there was no evidence that it had conducted adequate testing of the system.* Pertinently, while these lapses may have been more excusable before 1 July 2014, there is no excuse for the Organisation not to have initiated (and properly documented) a review of the system for compliance with the PDPA. *The responsibilities of ownership do not require technical expertise.*

[emphasis added]

27 Further, in *Re DS Human Resource Pte Ltd*,⁴⁷ the PDPC took the view that if an organisation does not have the requisite level of technical expertise to manage its IT system, the organisation may either procure technical expertise internally (eg, train its employees or hire individuals with the relevant experience) or engage competent service providers and give proper instructions.⁴⁸

28 Organisations must therefore be clear about the scope of services provided by their data intermediaries and service providers, make genuine attempts to articulate their business requirements, give proper instructions and exercise reasonable oversight over the measures carried out by their data intermediaries and service providers. The nature and extent of the services provided and the obligations of each party should be set out in the contract

47 [2020] PDP Digest 274.

48 *Re DS Human Resource Pte Ltd* [2020] PDP Digest 274 at [15].

and any instructions should be documented in writing prior to the provision of services.⁴⁹

B. From openness to accountability – Data protection policies and practices should be relevant and specific

29 As mentioned above, the PDPC’s pivot from compliance to an accountability-based regime in relation to the management of personal data is one of the most significant developments in Singapore’s data protection regime. This shift from compliance to accountability is reflected in the PDPC’s decisions as well.

30 In earlier cases, most of the organisations that breached the Openness Obligation (as it was known then) often did not implement *any* data protection policies or practices because they were not aware of their obligations under the PDPA.⁵⁰ However, it is clear from subsequent cases that it is not enough to just have some form of data protection policy – the policy must be relevant and specific to the organisation’s collection, use and disclosure of the personal data in its possession or under its control.

31 For example, in *Re Bud Cosmetics Pte Ltd*,⁵¹ the PDPC found the organisation in breach of s 12(a) of the PDPA because the privacy policy “only notified customers as to how the Organisation will use and process their personal data and *did not set out any procedures or practices as to how the Organisation and its employees should handle and protect the personal data in their possession or under their control*” [emphasis added].⁵²

32 Similarly, in *Re Xbot Pte Ltd*⁵³ (“Xbot”), the PDPC found the organisation to be in breach of s 12 of the PDPA, and noted that:⁵⁴

... although the Website and the App collected the same personal data for the same purpose, *the data protection policy published on the Website was*

49 *Re Smiling Orchid (S) Pte Ltd* [2017] PDP Digest 133 at [51]; *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [17].

50 Such as in *Re Jiwon Hair Salon Pte Ltd* [2018] PDP Digest 331 and *Re Singapore Cricket Association* [2019] PDP Digest 270.

51 [2019] PDP Digest 351.

52 *Re Bud Cosmetics* [2019] PDP Digest 351 at [17].

53 [2020] PDP Digest 292.

54 *Re Xbot Pte Ltd* [2020] PDP Digest 292 at [13].

expressly limited to personal data collected via the Website. This, in my view, is insufficient to meet the requirements of s 12 as users of the App would not have a clear indication of how their personal data would be handled by the Organisation. [emphasis added]

33 Significantly, the PDPC has clarified that regardless of their size, organisations should implement internal policies and practices, which should be communicated to employees. The size of the organisation is but one determinant of the complexity of the internal policies and practices required. The type and amount of personal data the organisation possesses and controls are other relevant considerations.⁵⁵ Therefore, even though there was only one employee (in addition to the sole director) in *Xbot*, the PDPC found that it should have developed internal policies and practices and communicated them to its employee.⁵⁶

34 The PDPC's findings in *Re Spize Concepts Pte Ltd*⁵⁷ also suggest that the scope of "policies and practices" required under s 12 could encompass contracts and documentation of an organisation's relationship with its data intermediary and, depending on circumstances, different "specific internal practices and policies" could be required.⁵⁸ The organisation did not have a contract or any documentation of its relationship with its data intermediary or any policies and practices relating to the transfer of its clients' personal data outside Singapore. The PDPC found that this was a breach of s 12(a), and the failure to produce them upon the PDPC's request was a breach of s 12(a)(i).⁵⁹

35 The PDPC's position in these cases is in line with its shift away from a "checkbox" compliance approach towards an accountability-based approach to managing personal data. Organisations should therefore ensure that their existing data protection policies and practices are able to demonstrate proper management and protection of personal data.

55 *Re Xbot Pte Ltd* [2020] PDP Digest 292 at [15].

56 *Re Xbot Pte Ltd* [2020] PDP Digest 292 at [15].

57 [2020] PDP Digest 311.

58 *Re Xbot Pte Ltd* [2020] PDP Digest 292 at [12]–[16].

59 *Re Spize Concepts Pte Ltd* [2020] PDP Digest 311 at [19]–[24].

C. *Approach to enforcement and financial penalties*

36 Generally, the quantum of financial penalty imposed by the PDPC is commensurate with various factors, such as the number of affected individuals and the sensitivity of the personal data.⁶⁰ The PDPC has said that it seeks to ensure that the financial penalty imposed is “reasonable and proportionate on the facts, the financial penalty should also be sufficiently meaningful to act both as a sanction and as a deterrent to prevent similar contraventions of the PDPA”.⁶¹ However, in comparison to the financial penalties imposed for breaches that occurred in the first few years after the PDPA was introduced when organisations may not have understood fully the manner in which they were required to comply with their obligations, the average quantum of the financial penalties imposed by the PDPC has gone up in recent years.

37 For instance, there was a significant increase in the number of organisations which received a financial penalty of \$10,000 or more. In 2019, a total of 26 organisations were directed to pay a financial penalty of \$10,000 or more (approximately 40% of all decisions published in that year). In contrast, a total of 17 organisations received financial penalties of \$10,000 or more in 2016, 2017 and 2018 combined.

Year	Number of organisations that received a financial penalty of \$10,000 or more
2016	4 ⁶²
2017	7 ⁶³
2018	6 ⁶⁴

60 For instance, in *Re Ninja Logistics Pte Ltd* [2020] PDP Digest 473 where a total of 1,262,861 individuals were affected, a \$90,000 financial penalty was imposed. In *Re Aviva Ltd* [2019] PDP Digest 145, even though only three individuals were affected, the organisation received a \$30,000 financial penalty because of the sensitive nature of the personal data affected and the fact that the organisation had previously encountered a similar incident.

61 *Re Horizon Fast Ferry Pte Ltd* [2020] PDP Digest 357 at [34].

62 Representing approximately 12% of all the decisions published that year.

63 Representing 28% of all the decisions published that year.

64 Representing approximately 18% of all the decisions published that year.

2019	26
2020	4 ⁶⁵ (as at 20 April 2020)

38 Against the backdrop of an increasing number of data incidents and complaints received by the PDPC and the potential increase in the volume of such reports upon the introduction of a mandatory data breach notification regime,⁶⁶ the PDPC has set out its new approach in deploying its enforcement powers to act effectively and efficiently on the increasing number of incidents in its *Guide on Active Enforcement* issued on 22 May 2019 (“Active Enforcement Framework”).

39 In addition to alternative dispute resolution mechanisms such as mediation and facilitated negotiations, the Active Enforcement Framework introduces two new options that are intended to motivate organisations to develop and implement accountable practices: (a) the option for organisations with sound accountable practices to submit an undertaking to implement their remediation plan and resolve the breach; and (b) the introduction of an expedited process for organisations that are contrite and prepared to admit liability.

40 As an incentive, the PDPC may accept voluntary undertakings and expedited decisions *in lieu* of full investigations, which will allow for faster resolution and potentially reduced penalties instead of a protracted fact-finding exercise.

IV. Concluding thoughts

41 Singapore has come a long way since 2012 when the PDPA was enacted. Having recognised the need to balance between the protection of individuals’ personal data and the benefits of allowing organisations to use personal data for data innovation purposes in today’s digital economy, since 2017 the PDPC has been taking steps for the PDPA to become a progressive data protection regime that promotes trust through the responsible use of data.

65 Representing approximately 33% of all the decisions published thus far.

66 Personal Data Protection Commission, “Public Consultation for Approaches to Managing Personal Data in the Digital Economy” (issued 27 July 2017).

42 With the coming amendments to the PDPA set to introduce enhancements to the consent regime, data portability and data innovation provisions, it is anticipated that the way in which the PDPC approaches the administration and enforcement of the PDPA will continue to evolve with the balance between data protection and data innovation expected to feature strongly.

IMPLEMENTING DATA BREACH PROGRAMMES: UNDERSTANDING NUANCES IN PRACTICE AND THE PERSONAL DATA PROTECTION ACT*

LIM Sui Yin, Jeffrey

LLB Hons (Bristol University);

Advocate and Solicitor (Singapore), Barrister-at-law (England & Wales)

I. Introduction

1 Proper design, implementation and execution of an executable, effective data breach management plan (“DBMP”) is a complex exercise. It requires a good grasp of the nuances of practical real-life conditions for each organisation, and of the potentially applicable standards or requirements.

2 Moreover, legal and regulatory standards (collectively, “DBM Standards”) can vary in applicability, scope, benchmarks, obligations and methods of notification or enforcement. As real-world conditions evolve, so do these standards – to keep up with the changing times. For instance, the Singapore Personal Data Protection Commission (“PDPC”) itself updated its *Guide to Managing Data Breaches*¹ (“GMDB”) in May 2019. In this regard, keeping a breach response programme current resembles the exercise of hitting a “moving target”, even where there is a degree of continuity between iterations of standards.

3 Whilst there may be variations in the details, terms or specifics, there is a general convergence of views as to what the overall structure and outline of a DBMP should be. An expression of this that is as good as any is the one contained in the GMDB itself, distilled into the four-step acronym “C.A.R.E.”² Indeed most literature in this space uses a similar breakdown

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

1 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019).

2 Broadly summarised as:

(a) contain the data breach which includes an initial assessment;

(continued on next page)

or phasing of steps although there may be variations in the terms of emphasis or details.³

4 Nonetheless, the application and execution of each of the four steps may involve addressing nuances when it is applied to comply with DBM Standards. Practical “on-the-ground” issues may give rise to particular difficulties if the DBM Standards applied are too prescriptive without being capable of application to different situations or circumstances, or too specific without being capable of flexibility of interpretation.

5 Since requirements imposed by DBM Standards can drive certain behaviours or responses by organisations to breach situations, it is important for the DBM Standards to have sufficient flexibility and adaptability to address different situations.

6 This article will discuss, by reference to the four steps of the C.A.R.E. framework under the GMDB, some issues which affect the design and implementation of DBMPs in the context of issues that DBM Standards address, taking into account some potential complexities, including practical issues and requirements that can arise. In doing so, a case will be made that in order for a DBM Standard to serve its stakeholders well, such a standard should have sufficient flexibility in interpretation or application to take into account real-life complexities.

II. Determining whether there is a breach

7 Although the GMDB begins with a discussion on containing the breach “whether suspected or confirmed”,⁴ it is useful to first consider certain potential nuances that might apply before an organisation even

-
- (b) assess the breach, which includes gathering the facts and evaluating the risks (including harm to individuals);
 - (c) report the breach to the Personal Data Protection Commission and/or affected individuals, if necessary; and
 - (d) evaluate the organisation’s response to the data breach incident.

3 The reader is referred to Appendix A of the NIST Special Publication 800-184 “Guide for Cybersecurity Event Recovery” by Michael Bartok *et al.* The version dated December 2016 was used as reference reading for the preparation of this article.

4 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 12.

concludes that there is a breach. In this regard, there are the twin problems of false positives (false alarms) and false negatives (undetected incidents). Each problem presents a different challenge of its own, and it is argued that a DBM Standard should address the potential impact of both.

8 False negatives do not, by definition, trigger an organisation to execute breach management steps. It is worth noting that for false negatives, one key issue is whether the organisation has undertaken reasonably sufficient and appropriate steps to verify that indications to them that there has not been an incident are reliable. This is a question of ensuring that there are appropriate internal breach reporting and surveillance mechanisms in place.

9 Asking a data protection officer or any manager to certify that there is no breach in place or that no breach has occurred would be difficult, not least because the difficulty would be akin to the difficulties in proving a negative, *ie*, proving the absence of something as opposed to proving its existence⁵ – although the application of a properly scoped audit with appropriate qualifications would be one potential way for such a statement to be given.

10 On the other hand, the problem of false positives is not insignificant, with industry articles indicating that there can be a high ratio of false positives to actual threats (let alone breaches).⁶ Additionally, recent studies⁷ have indicated that the resources which can be consumed in dealing with

5 The potential for zero-day exploits or historic but undiscovered security flaws adds to the difficulty of giving such a declaration. For an initial introduction to zero-day exploits, see “Security 101: Zero-Day Vulnerabilities and Exploits” *Trend Micro* (2 October 2019).

6 See Ajmal Kohgadai, “Alert Fatigue: 31.9% of IT Security Professionals Ignore Alerts” *Skyhigh* (19 January 2017), and in particular, in the context of cybersecurity cloud threats, the discussion of a 110:1 potential to actual threats ratio.

7 See “Ponemon Institute Reveals Security Teams Spend Approximately 25 Percent of Their Time Chasing False Positives; Response Times” *Bloomberg* (1 August 2019), referencing the joint study by the Ponemon Institute and Exabeam (the publication itself is only available through subscription). The key finding reported indicates that security personnel spend up to 25% of their time chasing false positives.

false positives can, in practice, be significant, and it has been noted that reactions to false positives can trigger “alert fatigue”.⁸

11 A specific problem presented by false positives in the context of compliance with a DBM Standard is the impact it has on the time taken to activate breach management processes. To begin with, the time taken to verify whether a particular incident is a false positive or is in fact a breach can be significant.

12 For instance, in the context of addressing false positives in matters of cybersecurity, the Anti-Malware Testing Standards Organization conducted an experiment in 2010 which involved the participation of seven vendors, and there the time spent (in man hours) for the same set of data ranged from 20 minutes to six hours.⁹ Variations in response time can be explained by differences in approach, the parameters used to conduct assessment, the context in which the information is presented and so on.

13 For this reason, executing a full breach protocol, including responding to specific DBM Standard timelines, based on mere discovery of a “suspected” breach may therefore be an impractical bar to hurdle, if not properly interpreted or provisioned with sufficient flexibility to allow for proper investigation. The timelines in a DBM Standard for reporting breaches to authorities and committing information in statements to third parties may well need to be tempered by a recognition of this issue,¹⁰ by

8 See Ryan Francis, “False Positives Still Cause Threat Alert Fatigue” *CSO* (3 May 2017), which also addresses some of the industry research findings on the issue, and certain best practices or issues, including common mistakes which lead to false positives.

9 See Anti-Malware Testing Standards Organization, *Guidelines to False Positive Testing* (2016). Additionally, the publication is a useful exploration of some of the complexities in respect of calibrating detection of breaches, including thoughts around prioritisation of detection parameters, itself a potentially complex area.

10 For an example of how a regulator has not proceeded with proposals for enacting rapid mandatory reporting timelines, see Marianne Kolbasuk McGee, “One-Hour Breach Reporting Rule Dropped” *Data Breach Today* (29 August 2013) where the US Department of Health and Human Services did not proceed with a one-hour breach reporting requirement for health insurance exchanges.

prescribing timelines that commence from such time as a breach can be ascertained with “a reasonable amount of certainty”, and not before.

14 These considerations should also, ideally, inform or shape any discussion concerning the application of any prescriptive obligations in DBM Standards as it relates to timelines. For instance, Art 33 of the European General Data Protection Regulation¹¹ (“GDPR”) prescribes that a data controller shall report the breach to the relevant national supervisory authority “without undue delay and, where feasible, not later than 72 hours after having become aware” of the breach.¹² Read in isolation, these qualifiers are important as questions could arise as to whether considerations concerning false positives or the work taken to ascertain and verify the existence of a breach could be elements that go into the question of what constitutes “undue” delay, issues of “feasibility” and the standard of “awareness” needed.

III. DBM Standards thresholds for action

15 In a similar way, if any DBM Standards were to have a hard (*ie*, definitive prescribed) deadline for reporting, it is argued that such a prescription should have appropriate qualifications which would allow room for applicability to meet different situations. It is in this light that any discussion of practical thresholds for reporting in DBM Standards must also delve into the question of not only the scale (*ie*, number of data subjects or volume of records affected) (“quantitative” thresholds), but also the quality of the data that is compromised (*eg*, whether the personal data is sensitive, the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, which could lead to harm) (“qualitative thresholds”).

16 At the outset it should be noted that quantitative thresholds almost necessarily involve a degree of arbitrariness. One issue is the problem of context. In a community of 100 individuals, a significant scale should be one person, whereas in a community of a million, this might well be 100. Even if one expressed scale in relative terms (expressed in percentages, for example), this might have practical and questionable outcomes. Drawing a

11 (EU) 2016/679; entry into force 25 May 2018 (hereinafter “GDPR”).

12 GDPR Art 33(1).

1% threshold of affected data subjects might seem low compared to a 10% threshold of affected subjects, but in a community of a million, this is a difference between 10,000 and 100,000 data subjects – relative measures tend to scale correspondingly.

17 However, the need for quantitative thresholds arises from the need for certainty. DBM Standards are intended to support the execution of specific and certain steps, with all its attendant usage of resources and efforts. Both leaders and administrators crave certainty and clarity. Quantitative thresholds provide not only decisiveness, but also defensibility against criticism. Effective policy-making further requires that such policies are capable of application in a manner that is consistent and implementable.

18 Qualitative thresholds, as defined above, might be considered as presenting the opposite issue of eschewing arbitrariness in favour of something less capable of certainty since the issue of likelihood of harm is a matter of assessment. From a legal and policy perspective, this has great attractiveness because it encourages a thinking and assess-the-situation approach, but it could present complications that business leaders and administrators may have difficulty articulating to their teams. The issue is whether it is feasible to empower individuals to competently make their own assessments of matters where such assessments themselves will be similarly assessed in post-mortems or legal forums (in the event of a dispute or investigation). An objective consensus needs to be formed around what standards are to apply and how they are applied.

19 To understand how qualitative thresholds might entail levels of complexity, it may be useful to consider what the key concept (“harm to the individual”) might entail.

20 On this point, it should first be apparent that not all “communities” of data subjects are homogenous. A community of unbanked economically-marginalised individuals would have a vastly different profile from high-net-worth individuals. One group might have limited or no financial data (or financial data of value), whilst the other might have exploitable and highly valuable data. One group might have limited healthcare records, and the other might have a surfeit of healthcare records. The exposure of financial data creates different levels and risks of “harm”.

21 Another observation is that an individual may be a part of more than one community. A patient who is HIV-positive might well form part of a larger community of healthcare patients, but the social, economic and

personal consequences of the exposure of all healthcare records of the larger community would have a markedly different impact on that individual as opposed to his “peer”.

22 Navigating concepts of likelihood of harm demands a nuanced consideration of the issue of context, and projections (or extrapolations) of consequences, and this in turn can also raise another issue of whether the risk of harm is fanciful or practical and real. For example, breaches and disclosures of information which appear, *ex facie*, less harmful might, on further investigation, reveal that there is greater severity of risk than originally anticipated.¹³ It is possible to overstate the complexities in this regard as there will be clarity of the potential for risk in some cases. In the examples discussed of financial and health information, it is fairly obvious that this is more likely than not to be information capable of resulting in harm if abused or misused.¹⁴

23 Provided that actions undertaken to verify the existence of a breach are pursued with due diligence, this timeline may need to have a degree of flexibility, or, alternatively, allow for progressive indications and the right to correct or update without prejudicing the liability of an organisation attempting to manage the situation.

24 Another alternative or complementary process is to allow an organisation to issue a “provisional notification” to a regulator, where it is possible to report an initial discovery that is being evaluated, and to allow that organisation to withdraw the notification if it is determined to be a false positive. This appears to be the option provided for in so far as

13 The reader is directed to the helpful discussion on factors affecting risk by the Office of the Victorian Information Commissioner in Australia at “Managing the Privacy Impacts of a Data Breach” (18 July 2019).

14 The Personal Data Protection Act 2012 (Act 26 of 2012) has no statutory definition or separate legal classification for “sensitive” personal data, but this has not prevented the Personal Data Protection Commission from articulating points of emphasis in relation to personal data that might be regarded as more sensitive than others. In practice, it would be difficult for any practitioner to ignore the reality that there is a difference in the potential for magnitude of liability between exposure of personal data *simpliciter* and sensitive personal data.

notification to the PDPC is concerned in respect of the right to provide an “interim notification comprising a brief description of the incident”.¹⁵

25 Where one draws the threshold of notification to a regulator would have real consequences in terms of resource consumption for all parties involved. Consider an organisation’s stakeholders involved in every notification exercise. Leadership should be placed on alert that a disclosure will be made. Public relations or customer relations teams should be ready to address the potential for disclosures to the public. Customer or data subject care teams may need to be ready to act to address an influx of requests (*eg*, requests to change passwords, system loads imposed on data-related requests, *etc*). Legal advisers need to be prepared and potentially weigh in on the situation, bearing in mind that there is potential for discovery in litigation or legal process. Reporting at any level will also impose resource burdens on the regulators themselves. Regulators will need to track the development of the situation – whether it is a false positive or not.

26 It follows that the issue is not only what thresholds for reporting or action might apply, but also the kind of expectations or standards required of parties once those thresholds have been crossed. On this point, if there is to be any gradation of thresholds for response, or gradation of the type of responses possible, there should also be corresponding clarity of the standards that apply. It would seem logical that a report of an unconfirmed breach should attract a different standard of follow-up action than one that is confirmed.

IV. C.A.R.E. framework – Containment

27 Given the variety of ways a breach might have occurred (IT and non-IT breaches included) the circumstances which led to the breach occurring, and the potential for a breach to have been a single *versus* an ongoing occurrence, it is understandable that the GMDB would not provide too specific or prescriptive a statement concerning standards by which an organisation would need to abide in terms of extinguishing or ceasing a particular breach.

15 See Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at Appendix B, p 36.

28 Since not all breaches are the same, the containment process may vary, and it would be practically difficult to be encyclopaedic about recommendations or guides concerning containment as a process. Indeed, what guidance there is in respect of containment is limited to five points stated in the GMDB.¹⁶

29 On the issue of actions undertaken during containment, the saying that hindsight is often “20-20” holds true, and various high-profile breaches have historically been reviewed in vigorous post-mortems, where observations on the standards regarding speed, diligence, reasonableness of response and other factors in the containment can sometimes be subject to scrutiny that unfairly imposes the benefit of hindsight so as to unfairly characterise omissions or actions taken in the “heat of battle” as lapses.

30 An example of a widely studied breach would be the Target Data Breach of 2013.¹⁷ Take, in that example, the application of the concept of a “kill chain”¹⁸ post-mortem analysis. The successful application of containment efforts in the kill chain doctrine is dependent on the level and availability of intelligence or information which would allow a security team to identify the ongoing attack so that containment or intervention can be applied. This dependency in turn suggests that the ability of an organisation to act credibly and effectively is always dependent on the access to information or evidence of an ongoing attack or vulnerability.

16 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 13, namely, isolate the compromised system or shut down the compromised system if necessary, prevent further unauthorised access to the system, isolate the causes of data breach, stop identified practices that led to the data breach, and establish whether lost data can be recovered and steps taken to minimise harm or impact.

17 The reader is encouraged to review the report issued by the US Senate Committee on Commerce, Science and Transportation titled “A ‘Kill Chain’ Analysis of the 2013 Target Data Breach” at <http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf> (accessed 1 February 2020).

18 Promulgated by defence experts Lockheed Martin, *ie*, where a defender of an organisation facing a malicious attempt to execute a data breach has the option to prevent the completion of a successful attack by interfering in any step in a malware attack. See also Lockheed Martin, “Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense”.

31 This in turn suggests that any standards that may be brought to bear in any DBM Standard should address the potential for a containment team to be acting under the proverbial “fog of war”, with limitations affecting how much a response team may know. Identifying and fixing one vulnerability may, on hindsight, not be complete if further information surfaces subsequently to indicate that a breach is in fact wider in scope than originally anticipated.

32 Determining when “containment” is at an end may therefore be a process. This is also recognised in the GMDB, where the indication is that the limitation of further damage at the stage of containment of a breach “will be dynamic as more facts are unearthed while investigating the incident”.

V. C.A.R.E. framework – Assessment and evaluation of breach

33 Indeed, the assessment phase of the C.A.R.E. framework also discusses considering certain aspects¹⁹ in respect of the breach in question, and it is noted that this information, or the accuracy or availability of this information, may well change in the process of assessment.

34 Take, for instance, an example where the initial discovery of a breach indicates that the personal data compromised is of, say, a limited number of data subjects, and with initial indications that the personal data compromised may be of trivial importance, with limited chances of harm to the data subjects. The initial information to an organisation would therefore be to encourage or direct the organisation to classify or treat the breach in a certain way, *ie*, making certain initial conclusions about the scale of the breach and the potential harm.

19 For example, the “types of personal data involved, the individuals whose personal data have been compromised, other contextual factors such as whether the data was publicly available”, *etc*, ease of identifying individuals compromised from the data, and circumstances of the data breach (whether the breach was by malicious intent, whether the data was sent to recipients who have no malicious intent or use for the data, *etc*) (Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at pp 15–17).

35 However, to say that this was an “initial” conclusion may be misleading. There may, at the time, be no actual information or indication that there would be any need for further assessment. The facts collected may appear conclusive, and the information may appear reasonably accurate with no specific reason to doubt the conclusions reached. “Initial” may not have been a reasonable characterisation of the information at the time.

36 Further information may only surface later to indicate that the scale of the breach, the type of personal data or the magnitude of harm might in fact be very different. If so, the organisation would then be required to “upgrade” its assessment of the severity of the breach. In these circumstances, it would appear unreasonable to hold an organisation to account for a failure to have treated the breach differently than initially thought.

37 Additionally, as with verifying a breach, the time taken in practice to contain a breach may be quite substantial²⁰ for this reason, and the containment process may still be underway when the need to execute an assessment arises. This is perhaps implicitly recognised in the GMDB which discusses a *preliminary* assessment during the containment process.

38 Indeed, the second phase in the C.A.R.E framework, “Assess”, is framed as proceeding “upon containment of the data breach”,²¹ and this is presumably continuing from the initial assessment. Because containment efforts can still be underway, it is argued that containment and assessment

20 The Ponemon Institute LLC has, yearly, conducted global analysis of data breach studies in conjunction with IBM, and, for comparison, the June 2016 study (available for download from IBM at <<https://www.ibm.com/downloads/cas/7VMK5DV6>> (accessed 1 February 2020)) identifies that the time taken to detect and contain a breach was 229 days and 82 days, respectively, for malicious and criminal attacks, and 162 days and 59 days, respectively, for breaches caused by human error. That figure is reported to have been increased in an updated 2019 report as 279 days to both identify and contain a breach, reported in trade literature (see “2019 Cost of a Data Breach Report” *ID Quantique* (10 September 2019)). The 2019 report can be accessed, subject to registration, at <<https://www.ibm.com/security/data-breach>> (accessed 1 February 2020).

21 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 15.

are not necessarily sequential, or neatly sequenced, and that DMB Standards should anticipate that these two phases can and do often overlap.

39 Notably, the time given under the GMDB to carry out assessment is not described in the assessment phase (step two) of the GMDB, but in the discussion as step three (“Report”),²² where organisations are expected “to carry out their assessment of the data breach expeditiously within 30 days from when they first become aware of a potential data breach”,²³ though this may well have been framed for the purposes of determining when decisions need to be made for reporting a breach.

40 It is argued that, for the nuances identified earlier, this “30 days” should be applied with appreciation of the potential for assessments to be affected by both the information that is only available within the 30 days (and information becoming subsequently available after 30 days), and the practical limitations in time taken to execute the assessment and containment.

41 Similar considerations apply in respect of the “Evaluate” phase of the C.A.R.E. framework.²⁴ Not all the forensic work or the gaining of secondary insights drawn from the study of the breach can be contained within the first report or completed within the deadline to deliver a final report. Investigations might well in fact continue after any such report issuance or report timeline. Indeed, the understanding and the perspectives of a particular breach can evolve.

42 To illustrate, assume that an organisation has suffered a data breach. It may be that the first fully formed conclusions drawn from a fully completed evaluation may be that the data breach was due to a particular flaw in a software component. The evaluation then sets off a chain of actions including ensuring that the vendor that delivered the software duly updates or corrects the flaw. It might then subsequently emerge that though the flaw was in fact present, the exploitation of it was part of a large pattern of conduct by a bad actor, including inserting and executing malware in the organisation’s system that harnessed or perhaps “weaponised” the flaw.

22 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.

23 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.

24 See also the earlier discussion at para 29 above.

43 This type of information might not be immediately apparent. Further evaluation might reveal new information, such as whether there were any traces or records which explain how the flaw was exploited. There might an “inside job” detected. Initial blame might have been wrongly cast or at least not correctly apportioned. Time may need to be spent to ensure that the correct evaluations are formed. Evaluation (and, for that matter, assessment) might, by its nature, be an iterative process – learning from the first report, and then issuing a second, and so on.

44 This is also a question of what the focus of the evaluation can be. Certain priorities can be the first issues formulated “right out of the gate”, but then change and shift subtly as more information is gathered. An organisation might start thinking that the issue is the capacity for or risk of the occurrence of the data breach, and then find that the true issue is the capacity (or lack thereof) for responsiveness and effectiveness in addressing situations. The focus might shift when things are clearer, and different learnings can crop up.

45 The nuance here therefore is that if DBM Standards are applied with a view to determining whether an organisation has executed its containment and assessment efforts adequately to meet standards or expectations, such an analysis should be applied or tempered with the caveat that organisations should be given opportunities to explain or justify their actions based on the limitations of available information *at the time that a breach unfolds*. There should be interpretive flexibility over any standards that may apply or be brought to bear.

VI. C.A.R.E. framework – Reporting

46 The third stage of the C.A.R.E. framework under the GMDB is the reporting phase. The issues discussed above – the availability of intelligence, time taken to contain and assess a breach, and the potential for initial information to be inaccurate or inadequate, *etc* – all provide practical implications to what then can be expected in a report. There are, in particular, two issues where these nuances could affect the reporting phase of the C.A.R.E. framework, namely time to report and the obligation to notify the PDPC and/or the affected data subjects.

47 In terms of time to report, it is noted that, in addition to the expectation that an assessment should be made within 30 days from when

an organisation is first aware of a potential data breach, the GMDB also prescribes a fixed time frame as to what constitutes “undue delay” in respect of references in the GMDB – *ie*, “a period no longer than 24 hours” – first referenced in the context of reporting by data intermediaries to their client organisations.²⁵ There is no use of the defined term of “undue delay” in any other context in the GMDB.

48 In terms of the obligation to notify the data subject, the GMDB requires organisations to consider the risks associated with whether the breach is of significant harm, or significant scale,²⁶ with a 72-hour notification window “after establishing that the data breach” is likely to be of significant harm or significant scale,²⁷ with a proviso that organisations which are uncertain as to the need to notify data subjects are to seek clarification from the PDPC.

49 It is then stated in the GMDB that notifications (or the lack of notifications) “will affect the PDPC’s decision as to whether an organisation has reasonably protected the personal data in its possession or under its control”. For context, the requisite information, factors to consider, and information to be provided to the PDPC are not unprecedented and have some degree of similarity or equivalence with considerations articulated in other laws.²⁸

50 In this regard, it should be noted that notifications to individuals are considered against the framework of whether there is the likelihood of significant harm or impact, and whether notification to individuals would

25 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 20.

26 Point 1 of the five points of notification (Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.)

27 Point 3 of the five points of notification (Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.)

28 Article 33 of the GDPR is an example, where Art 33(3) requires reporting of the nature of the personal data breach, categories and approximate number of data subjects concerned (including number of records), the contact details of the data protection officer or other contact point where information can be obtained, the likely consequences (*eg*, harm) of the personal data breach, the measures taken or proposed to be taken by the data controller to address the breach, including, where appropriate, measures to mitigate possible adverse effects.

help individuals undertake self-help actions (*eg*, changing of passwords) – this is indicated in the GMDB.²⁹ Notification to the PDPC is based on either whether there is the likelihood of significant harm or impact, or the scale (a figure of 500 affected individuals acting as an indication of significant scale).

51 The question of how to provide an opportunity for data subjects to undertake self-help is situation specific. Examples of steps in terms of self-help that are given in the GMDB include reviewing suspicious account activities, cancelling credit cards and changing passwords. Notifications might also be supplemented by suggested practical guidance to affected individuals as to what steps the individual should also be taking, though any advice or guidance should be undertaken with care, *ie*, be carefully and simply worded so as not to be misunderstood or misapplied.

52 However, in practice, there is always a degree of risk of personal liability that would attend any communications issued in respect of a breach. The “fog of war” in a developing situation may not permit the organisation to be too accurate or comprehensive, and this should be a relevant consideration in mitigating liability risks. If information is wrong, for example, disclosure might have the effect of causing panic or raising false alarms. If information is necessarily inadequate due to circumstances, it may have little value other than to raise tension and anxiety.

53 Any DBM Standard that holds organisations to high standards of care of notification without appropriately discounting for the proverbial “unknown unknowns” or the fact that knowledge might be imperfect might only encourage retentiveness (from an abundance of caution) at a time when, from a policy perspective, fuller disclosure may in fact be desirable. This can result in balancing exercises where it is not always obvious that erring on the side of disclosure may be legally sound.

54 Notification to data subjects does, however, represent a significant step forward in terms of managing the liability of the organisation – it is in the context of data subject notification that the first information going out may facilitate a data subject’s consideration of whether to exercise a right to

29 See point 2 at p 18 of Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019).

take action. Additionally, issues may arise in respect of whether the notification was properly executed – including whether there is a reasonable standard of care concerning the information shared by the organisation.

55 As with reporting to the PDPC, it is noteworthy that the GMDB also contemplates the potential for an interim notification comprising a brief description of the incident to be used.³⁰ Given the potential for the existence of the “fog of war” as earlier identified, it is submitted that this is not only salutary but may be worth considering whether it could be expanded on.

56 Specifically, it may be useful to consider whether to allow for a degree (if only limited) of legal immunity³¹ to the organisation against private claims by third parties concerning liability for the potential for incorrect or incomplete information given at the outset, in recognition of the potential for new information or subsequently identified information to contradict or significantly qualify interim information.

57 Such a proposal could also be balanced by expressing that such immunity is subject to the organisation issuing such information in good faith and applying reasonable diligence in doing so. Such an arrangement, it is submitted, would help encourage organisations to share as much information as they can.

VII. Conclusion

58 There are other factors and issues concerning data breaches which are beyond the scope of this article to investigate or survey, and this is not intended to stand as a comprehensive discussion of all considerations that may affect the application of the C.A.R.E. framework in respect of data breaches.

59 Examples of issues that also have further implications for managing data breaches include the potential for legal claims by third parties, discoverability of communications, the impact or availability of insurance

30 See Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at Annex C, p 37.

31 Indeed, since the initial draft of this article, the writer notes that s 12 of the Personal Data Protection (Amendment) Bill 2020 was published, and that it proposes just such a form of limited immunity in the proposed s 26D(8)

cover, and the need to co-ordinate disclosures across borders. Indeed, on the issue of cross-border disclosures and the impact of DBM Standards under foreign laws, the interesting question of whether there is a case to call for compatibility, if not convergence, of standards deserves further investigation.³²

60 Even in a strictly domestic setting, it would also be useful to consider to what extent alignment of standards under the PDPC with other sector-specific laws in Singapore may be available or should be undertaken.

61 Within the relatively “small sample size” of issues raised, it is submitted that there is already enough potential for complexity to justify both the careful calibration of DBM Standards and their flexible application. In this regard, the GMDB is a sound starting point, and it is submitted that further evolution or development of the standards for breach management in this regard should continue to amplify and elaborate on this potential to provide for flexibility and adaptability.

32 For a snapshot of how complex the variations can be across jurisdictions on the issue of data breach notifications, and a call for alignment, a useful publication issued in 2019 is the publication commissioned by the US Chamber of Commerce, by Messrs Hunton Andrews Kurth, “Seeking Solutions: Aligning Data Beach Notification Rules Across Borders” at <<https://www.huntonak.com/images/content/5/6/v2/56941/Data-Breach-Notification-paper.pdf>> (accessed 1 February 2020).

LESSONS ON MANAGING BREACHES IN SINGAPORE FROM ONE YEAR OF THE GENERAL DATA PROTECTION REGULATION*

Bryan TAN

Partner, Pinsent Masons MPillay

I. Introduction

1 A mandatory breach notification (“MBN”) regime is set to be introduced soon in Singapore, as the Personal Data Protection Commission of Singapore (“PDPC”) has repeatedly affirmed its inclusion in coming amendments to the Personal Data Protection Act 2012¹ (“PDPA”).² This development is in line with international developments, as jurisdictions like Canada, Australia and Europe have implemented breach notification obligations,³ albeit with different standards.

2 Currently, the “gold standard” is the European Union (“EU”) General Data Protection Regulation⁴ (“GDPR”), which has been in effect since 25 May 2018. The GDPR requires data controllers to notify a supervisory data authority (“SDA”) of a personal data breach within 72 hours of becoming aware of it, and non-compliance can lead to severely large financial penalties. As a result, numerous data breaches have been reported in all EU jurisdictions since the beginning of the GDPR’s

* The author wishes to acknowledge assistance rendered by Sarah Lim for this article. Any views expressed in this article are the author’s personal views only and should not be taken to represent the views of his employer. All errors remain the author’s own.

1 Act 26 of 2012.

2 Yeong Zee Kin, Deputy Commissioner for Personal Data Protection, keynote speech at “Know Ahead to Stay Ahead – Leadership’s Engagement in Data Protection” (22 May 2019).

3 Australia’s mandatory breach notification came into effect on 22 February 2018, with amendments to the Privacy Act 1988 (Cth). Canada’s mandatory breach notification regime is contained in the Personal Information Protection and Electronic Documents Act (SC 2000, c 5) since 1 November 2018.

4 (EU) 2016/679; entry into force 25 May 2018 (hereinafter “GDPR”).

operation. This has also allowed for a significant amount of data to be collected regarding data security incidents.

3 Singapore businesses have raised concerns about their unfamiliarity with implementing policies and measures in accordance with the requirements of the data breach notification regime.⁵ Whilst the PDPC has released an updated *Guide to Managing Data Breaches 2.0*⁶ in alignment with the coming MBN regime, there is still plenty to be learnt from the first year of the GDPR. This article draws observations from EU data and makes recommendations on how Singapore businesses could prepare for the coming mandatory breach regime.

II. Data trends in the European Union

4 The EU data examined is drawn from a new report issued by Pinsent Masons,⁷ which features data from a large number of active data security matters handled by Pinsent Masons from January 2018, and freedom of information requests gathered from data protection authorities across Europe. Two overarching observations can be made: first, a significant 47% of breach notifications were made late, *ie*, after the required 72-hour time frame. Second, there was a noteworthy spike in breach notifications after the GDPR came into force. The second observation does not apply wholesale to all EU jurisdictions; rather, the Netherlands, UK and Ireland have seen the largest spike.⁸ One possible reason for this is that English-speaking countries pose more attractive targets to attackers. An alternative reason is that organisations from these countries comply more strictly with GDPR obligations and are better equipped internally to report data breaches. However, a significant issue possibly contributing to the spike is “over-reporting”. The Pinsent Masons data, as well as the UK Information

5 Personal Data Protection Commission, “Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy” (1 February 2018) at p 10.

6 Published 22 May 2019.

7 “Report Flags GDPR’s Impact on Data Breach Notification” *Pinsent Masons Out-Law News* (11 June 2019).

8 For instance, the UK Information Commissioner’s Office went from under 400 personal data breach notifications in April 2018 to a monthly average of 1,276 notifications.

Commissioner's Office ("ICO") itself,⁹ has affirmed that the ICO received a high level of reports that are not actually caught by the mandatory reporting obligation.

5 These trends and the phenomenon of over-reporting can be attributed to organisations' inadequate post-breach actions, particularly their data review and incident response measures. This section discusses how these measures have proved deficient, and how they have contributed to the overarching trends.

III. Inadequacy of post-breach actions

A. *Current data review measures*

6 Under the GDPR, personal data breaches do not need to be reported if they are "unlikely to result in a risk to the rights and freedoms of natural persons".¹⁰ Thus, when a personal data breach occurs, organisations must swiftly conduct a risk assessment on whether the exposure of this data can result in the harm of individuals' rights and freedoms. Such findings should be fed into any notification decisions and related notification submission narrative, so that in serious cases, data subjects can be notified and then take steps to protect themselves and/or to mitigate any risk.

7 The assessment necessarily involves first determining the extent of the data affected and then considering the degree of harm the affected data might result in, *ie*, how "sensitive" the data is.¹¹ Sensitivity can be categorised into different levels. For instance, names and e-mail addresses can be understood as "Level 1" personal data which is unlikely to pose

9 See "ICO Warns on Over-Reporting of Data Breaches" *Pinsent Masons Out-Law News* (13 September 2018).

10 GDPR, Art 33, para 1.

11 Lanx Goh & Nadia Yeo, "Sensitive Personal Data in the Singapore Context?" [2019] PDP Digest 37 at 43.

significant harm, as opposed to “Level 2” data like NRIC numbers.¹² However, the context of the incident and the relationship of the individuals to the data and to the organisation are also highly relevant when reviewing the risk of harm the data represents.

(1) *Impact of inadequate data review measures*

8 The difficulty of the data review process has resulted in a spike in the number of precautionary notifications to SDAs, and thus notifications as a whole. Breaches that involved only “Level 1” data made up 42% of all UK data security incidents, but a majority of these “Level 1” breaches (58%) were reported to the UK ICO, generally because the organisation struggled with the data review process and was unable to conclude that a risk of harm to data subjects was unlikely. As noted above, inadequate data review measures also resulted in great cost to organisations.

9 Because of this complexity, organisations have struggled to effectively analyse the risk posed by the affected data within the 72-hour time frame. Based on the incidents witnessed in Singapore, this is a pertinent issue for small and medium enterprises (“SMEs”) and “business to business” (“B2B”) focused companies due to the typically unstructured nature of their data storage. For instance, their internal systems may store various data in personal folders in an *ad hoc* fashion. As a result of this, the data review process can be especially complex, time-consuming and therefore costly for these businesses. This is not helped by the fact that organisations are generally unprepared for addressing a data breach and thus struggle with their inexperience. Organisations will do well to conduct pre-breach preparations including desktop and cyber-range simulation exercises to familiarise themselves with the data review process.

12 NRIC numbers can be used to identify the individual and can be used to access large amounts of information relating to the individual. They are therefore of higher sensitivity/risk than an e-mail address. See Personal Data Protection Commission, *Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers* (updated 26 August 2019) at p 6.

B. Current incident response measures

10 Key elements in the successful mitigation of a breach's effect are the formation and mobilisation of a dedicated and experienced incident response team ("IRT"). Pinsent Masons found inadequacies in both aspects. First, in regard to formation, IRTs should comprise both external advisers (usually IT forensics, public relations and legal) and internal stakeholders. In reality, organisations tend to neglect the involvement of senior internal decision-makers (eg, board members) in IRTs. Secondly, in regard to mobilisation, it is best practice for organisations to fully plan, rehearse and prepare for the deployment of an incident response plan following a data breach. The mobilisation of an IRT is a critical step in controlling and containing the repercussions of a breach. However, the reality is that, often, organisations neglect to produce or maintain such plans.

11 Another pertinent mobilisation issue is the late deployment of a legal team. Although 40% of instructions were within one to three days of detection, 39% of all incidents involved the instruction of legal counsel as external counsel more than ten days after detection. On average, organisations took over nine days to instruct legal counsel following breach detection, with more than 18% taking over 50 days.

(1) Impact of data response measures

12 The inadequate formation and mobilisation of IRTs, particularly senior internal decision-makers' non-participation in receiving and sharing information, and lack of input in response decision-making, has led to more lengthy, costly and ineffective incident responses. These lengthy response measures contributed strongly to late notifications; more precisely, the data indicated that the primary contributory factor to late notifications was organisations' delays in reporting breach incidents to their legal advisers or other independent incident-response experts. This is concerning considering the penalties that SDAs can impose given non-compliance with the notification obligation.

13 Furthermore, the late deployment of legal experts can lead to the organisation taking unnecessary if not detrimental steps on its own, which may further lengthen and increase the cost of the response process. For instance, the report found that a significant 25% of ICO cases were notified to the ICO by organisations themselves. Organisations usually give the ICO an incomplete account of the breach incident and response. This is

more likely to result in lengthy ICO investigations that draw an organisation's time and effort away from crucial technical investigations which would otherwise ensure the full effects of the breach are known and contained.

IV. The coming Singapore mandatory breach notification regime

14 The coming MBN regime the PDPC is set to introduce notably sets equally stringent requirements as the GDPR's. The proposed PDPA regime will give up to 30 days for organisations to assess a potential data breach once they become aware of it.¹³ Once the organisation assesses the breach to be:¹⁴

- (a) likely to result in significant harm or impact to the individuals to whom the information relates; or
- (b) of a significant scale (*ie*, more than 500 individuals' personal data is affected),

then it is obliged to notify the PDPC as soon as practicable, no later than 72 hours from the time the breach is ascertained to be reportable. If the breach is assessed to be likely to cause significant harm or impact to affected individuals, then those individuals should be informed *as soon as practicable* (*ie*, there is no definitive 72-hour window).¹⁵ This is to allow individuals the opportunity to take steps to protect themselves from the risks of harm or impact from the data breach.¹⁶ The GDPR has a similar obligation,¹⁷ but the report's data showed only 32% of incidents resulted in the notification of individuals, as most incidents were not serious enough to invoke the obligation.

13 Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (1 February 2018) at p 12.

14 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.

15 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at pp 12–13.

16 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 18.

17 See Art 34 of the General Data Protection Regulation (EU) 2016/679.

15 The similarities between the regimes suggest that there is value in drawing lessons from the experiences of EU organisations thus far.

V. Assessing and addressing future challenges for Singapore businesses

16 Following the trend represented by the results of the GDPR's MBN regime, the implementation of Singapore's regime will inevitably lead to a spike in breach notifications in Singapore. As outlined above, EU organisations' preparations for the MBN regime have proved inadequate. This is in spite of the EU having a long-established data protection regime since 1995, in the form of the EC Directive 95/46/EC ("Data Protection Directive"). Conversely, Singapore has only had data protection regulations for the last seven years. With a shorter history of compliance with data protection laws, Singapore businesses are likely to face even more difficulty with implementing measures and policies in alignment with the coming regime. Furthermore, the PDPC is known to be a particularly proactive SDA – and increasingly so, considering that it issued 51 reported decisions in 2019, a significant jump from 29 in 2018 and 19 in 2017. Another factor to consider is the fact that Singapore is an English-speaking jurisdiction, which may mean it is an attractive target for attackers as suggested by the GDPR experience.

17 Thus, taking into account the situation in Singapore, any Singapore business that collects the personal data of its customers and staff should be concerned about preparing for the coming MBN regime. Businesses which offer online services, or store customer or staff information online, are particularly vulnerable. The reported 2019 PDPA decisions showed that a variety of businesses, including retailers and food and beverage businesses,¹⁸ human resource consultancies,¹⁹ tuition agencies²⁰ and cryptocurrency firms,²¹ breached the PDPA due to poor security measures. A majority of these businesses failed to have adequate data protection

18 *Re Bud Cosmetics Pte Ltd* [2019] PDP Digest 351; *Re Spize Concepts Pte Ltd* [2020] PDP Digest 311.

19 *Re DS Human Resource Pte Ltd* [2020] PDP Digest 274.

20 *Re Tutor City* [2020] PDP Digest 170.

21 *Re InfoCorp Technologies Pte Ltd* [2020] PDP Digest 282.

policies within themselves, further highlighting the vulnerabilities of Singapore businesses.

18 Lastly, but perhaps more importantly, SMEs should be cautious in view of the great danger they face. The PDPA has highlighted that SMEs “should not take the security of their website for granted simply because of the smaller scale of their businesses”;²² instead, considering their significant vulnerability to targeted cyberattacks,²³ and the frequency of inadvertence leading to data breach incidents,²⁴ SMEs should be concerned by their current little to no investment in cybersecurity measures likely resulting in breaches of the PDPA. Accordingly, this section will give recommendations on what businesses can learn from the EU experience, and advise further on additional challenges that may be faced in the Singapore context.

A. Prepare internal and external resources

19 As discussed above, data review measures are relevant where the parameters of the breach are unclear. In Singapore, where many reported personal data breaches occur due to “lack of access controls ... system design errors and human error”²⁵ (*ie*, inadvertence), the data affected by the incident may seem easier to determine, thus making data review measures ostensibly of less importance. Nonetheless, to say that intentional cybercrime is less prevalent in Singapore would be extremely presumptuous. The seemingly lower prevalence of broad data attacks may very well be linked to businesses’ inadequate breach detection tools. Thus, it should still remain a prerogative of businesses to improve their data review measures, should a broad data breach occur, so as to reduce the time and cost of investigations, and ensure compliance with the notification time frame. Also relevant to this is the obligation to notify affected individuals, which has an even stricter time frame. It may also be in the interests of businesses to reduce the number of precautionary breach notifications to the PDPC by assessing incidents in not only a timely manner but with more accuracy, so

22 *Re Tutor City* [2020] PDP Digest 170 at [26].

23 Cyber Security Agency of Singapore, “Singapore Cyber Landscape 2017” (2018) at p 12.

24 *Re Tutor City* [2020] PDP Digest 170 at [26].

25 *Re Tutor City* [2020] PDP Digest 170 at [26].

that the PDPC can dedicate more resources to promptly assisting serious breach incidents.

20 Improving data response measures is also crucial. As similarly required by the GDPR, the PDPC will require a detailed breach notification report, including the extent, nature and causes of the data breach; similar requirements apply to the affected individual obligation.²⁶ Preparing an adequate incident response team and plan will assist businesses in meeting their obligations as swiftly as possible, thus avoiding unnecessarily long PDPC investigations that consume businesses' resources and funds. Deploying a legal team early could allow organisations to better understand, and take steps to ensure compliance with, all their legal obligations at an early stage. This will help organisations minimise legal liability and reduce future financial costs from potential penalties and claims.

21 Nonetheless, developing these measures in the Singapore context is easier said than done. Considering businesses' lack of experience with data protection laws, external assistance from independent data protection experts is likely to be necessary for many. Businesses should consider whether it would be appropriate to prioritise seeking and engaging data protection experts from IT and legal organisations before the regime is enacted, considering Singapore's limited landscape and the resource crunch that is likely to occur post-implementation of the regime.

B. Consider restorative measures to affected individuals

22 Remedial actions taken by organisations post-breach continue to be a mitigating factor towards the determination of PDPC directions.²⁷ However, these remedial actions have been limited to the prevention of further unauthorised access to personal data, in other words, containing the effects of the breach. This leaves the damage that affected individuals have already incurred through the loss of their personal data completely unaddressed. It is pertinent to note that the direction to "take steps to

26 Personal Data Protection Commission, *Guide to Managing Data Breaches 2.0* (22 May 2019) at p 19.

27 See at *Re InfoCorp Technologies Pte Ltd* [2020] PDP Digest 282 at [16]; *Re Learnaholic Pte Ltd* [2020] PDP Digest 387 at [24]; *Re DS Human Resource Pte Ltd* [2020] PDP Digest 274 at [18]; and *Re GrabCar Pte Ltd* [2020] PDP Digest 252 at [24].

protect themselves from the risks of harm or impact from the data breach” may be no more than a vague and unhelpful instruction for affected individuals; the data is already lost, and little can be done to personally mitigate the effects of an extracted residential address or NRIC number. With the advent of the MBN regime, and therefore a spike in notifications and reported decisions, there is a possibility that individuals will grow more aware of and concerned about the value and safety of their personal data. Remedial actions in terms of breach containment may satisfy the PDPC, but it is ultimately affected individuals who face the greatest danger, and thus have the greatest stake at risk, in the event of a breach incident. It is therefore important for businesses to consider what restorative action²⁸ – beyond mere notifications – individuals may expect from businesses who mishandle their data, and to prepare for them accordingly.

VI. Conclusion

23 Working to comply with the coming MBN regime may be perceived to be a financial burden to some businesses, but it ultimately has social utility to Singapore businesses and society. Cybersecurity and data protection are two sides of the same coin; businesses, being prone to data attacks themselves, will benefit from the lessons learnt from reported cases, and the increased protection and safety of improved cybersecurity. Furthermore, as Singapore businesses expand and participate in more cross-border transactions, the PDPA regime and the assistance rendered by the PDPC will prove helpful to businesses taking steps towards compliance with the laws of overseas jurisdictions. Data has shown that the first year of the GDPR has proved difficult for organisations, but Singapore businesses should take this opportunity to glean lessons from their failures – to adapt and ultimately strengthen their own well-being.

28 Examples of restorative action would include customer helplines, credit monitoring services, steps taken to secure copies of the stolen data, and dark web monitoring (for the stolen credit card numbers and identities).

THE PERSONAL AND DOMESTIC EXCLUSION*

Benjamin WONG YongQuan[†]

LLB (National University of Singapore);

Advocate and Solicitor (Singapore)

I. Introduction

1 Personal data processing activities that are characterised as “personal” or “domestic” are usually excluded from the scope of data protection law. This exclusion, which will be referred to in this article as the “personal and domestic exclusion”, is a common feature of data protection laws around the world.

2 The rationale for the personal and domestic exclusion, it is suggested, is that it would be unduly oppressive to impose data protection obligations on individuals acting in a personal or domestic capacity. For example, everyday conversations frequently revolve around people, and it would be excessive to require notification and consent before personal data is disclosed in the context of such conversations. It would similarly be excessive if personal records made about other people (for instance, lists of birthdays and home addresses) were subject to the security, access and correction obligations under data protection law.

3 The Singapore Personal Data Protection Act 2012¹ (“PDPA”) imposes data protection obligations on individuals (among other types of organisations).² However, the PDPA also contains a personal and domestic

* 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 are the author’s own.

† Sheridan Fellow, National University of Singapore.

1 Act 26 of 2012.

2 See Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1). For a recent example of an individual being found liable for breach of the Personal Data Protection Act, see *Re Amicus Solutions Pte Ltd* [2020] PDP Digest 404.

exclusion, set out in s 4(1)(a).³ Section 4(1)(a) provides that Pts III to VI (which contain the provisions imposing data protection obligations) “shall not impose any obligation on ... any individual acting in a personal or domestic capacity”. As such, individuals acting in a personal or domestic capacity are exempt from the data protection obligations of the PDPA.

4 The purpose of this article is to examine and clarify the scope of the personal and domestic exclusion under s 4(1)(a). It will also consider how s 4(1)(a) applies in the context of individual use of social media.

II. Application of the section 4(1)(a) exclusion

5 From the legislative language of the PDPA, it is clear that there are two limits to the scope of s 4(1)(a). These two limits are considered below.

A. First limit: “individual”

6 First, the s 4(1)(a) exclusion applies only to *individuals*. An “individual” is defined in the PDPA as a “natural person”; as such, s 4(1)(a) does not apply to juridical persons such as companies, which cannot rely on s 4(1)(a).⁴ This limit is reasonably clear and unambiguous, and nothing more on it need be said here.

B. Second limit: “acting in a personal or domestic capacity”

7 Second, s 4(1)(a) only applies where an individual is *acting in a personal or domestic capacity*. If an individual is not acting in a personal or domestic capacity, then he will generally be obliged to comply with the data protection obligations of the PDPA.⁵

8 While it is often quite obvious when an individual is (or is not) acting in a personal or domestic capacity, there are cases where it is not obvious.

3 Section 4(1)(a) of the Personal Data Protection Act 2012 (Act 26 of 2012) is part of a range of organisation-specific exclusions: see Benjamin Wong, “Data Privacy Law in Singapore: the Personal Data Protection Act 2012” (2017) 7 *International Data Privacy Law* 287 at 291.

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

5 See *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [9].

This is because the phrase “acting in a personal or domestic capacity” is open to a range of plausible interpretations. This article turns to examine the meaning of “acting in a personal or domestic capacity”, in the light of the legislative wording of the PDPA and the guidance provided by the Personal Data Protection Commission (“PDPC”) in its guidelines and decisions.

(1) “Personal” and “domestic”

9 As a starting point, the meaning of the words “personal” and “domestic” in s 4(1)(a) should be considered.

10 The word “personal” is not defined in the PDPA, but the PDPC has stated in its advisory guidelines that “[a]n individual acts in a personal capacity if he or she undertakes activities for his or her own purposes”.⁶

11 The word “domestic” is defined in the PDPA as “related to home or family”.⁷ According to the PDPC’s advisory guidelines, an individual “acts in a domestic capacity when undertaking activities for his home or family”, for example, when “opening joint bank accounts between two or more family members, or purchasing life insurance policies on one’s child”.⁸

(2) “Personal or domestic” versus “business or work”

12 A useful distinction may be drawn between acting in a personal or domestic capacity, and acting in a business or work capacity.

13 First, it is clear that individuals acting in a business capacity do not benefit from s 4(1)(a). The PDPC’s decision of *Re Sharon Assya Qadriyah Tang*⁹ illustrates this point. Here, the respondent was an individual who had purchased “leads” in the course of her work as a telemarketer. A lead would typically comprise an individual’s name, NRIC number, mobile phone number and annual income range. The respondent subsequently

6 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) at para 6.9.

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

8 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 9 October 2019) at para 6.10.

9 [2018] PDP Digest 319.

sold the leads to other persons, in order to supplement her income. In so doing, the respondent had disclosed personal data without providing notification or obtaining consent, and was therefore held to have breached the PDPA.

14 In determining whether the respondent was obliged to comply with the data protection obligations of the PDPA, the PDPC noted that “the converse of a person acting in a personal or domestic capacity is one that acts in a business capacity”, and the respondent in this case had been acting in a business capacity when she bought and sold leads.¹⁰ Accordingly, the PDPC found that the respondent was “clearly not acting in a personal or domestic capacity in respect of the buying and selling of leads”.¹¹

15 Second, there is support for a distinction between individuals acting in a personal or domestic capacity and individuals acting in a work (or professional) capacity. Reference may be made here to the recent PDPC decision of *Re Grabcar Pte Ltd*.¹² This case involved the “Grab App”, a mobile ride-sharing application. The Grab App provided a carpooling function known as “GrabHitch”. The GrabHitch function would connect a passenger with a driver, who would give the passenger a ride to the passenger’s destination on the way to the driver’s own destination. Two passengers, who had used GrabHitch, made separate complaints to the PDPC, alleging that their GrabHitch drivers (the “Drivers”) had published their personal data on social media platforms without their consent.

16 The PDPC found that GrabHitch drivers generally provided carpool rides in their personal capacity, and the Drivers therefore could not have been in breach of the PDPA.¹³ This finding was made in view of the fact that “GrabHitch drivers provide carpool rides on a non-commercial and non-profit basis” – both the relevant subsidiary legislation and the GrabHitch Code of Conduct mandated that GrabHitch drivers could only receive payment from their passengers on a cost-recovery basis.¹⁴ In addition, GrabHitch drivers were not permitted to solicit for passengers, had to ensure that their carriage of passengers was incidental to their use of

10 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [10].

11 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [10].

12 [2020] PDP Digest 252.

13 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [15].

14 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [10]–[12].

their vehicles, and could only offer two carpool trips per day.¹⁵ The PDPC emphasised that GrabHitch drivers were engaging in an essentially private activity, “as compared to professional GrabCar drivers”.¹⁶

(3) *Requirement of consistency*

17 Section 4(1)(a) does not expressly specify that an individual must have been acting *purely* in a personal or domestic capacity, in order to be exempted from the data protection obligations of the PDPA. Nonetheless, the enforcement decisions of the PDPC make it clear that, for an individual to take advantage of s 4(1)(a), he must have consistently acted in a personal or domestic capacity. Two enforcement decisions by the PDPC illustrate this requirement of consistency.

18 In *Re Chua Boon Yong Justin*,¹⁷ the respondent was a registered property agent, to whom the complainant and his wife had provided their names and NRIC numbers, for the purposes of entering into a tenancy. The complainant and his wife subsequently fell into dispute with another tenant, Ms C. At her request, the respondent provided Ms C with the names and NRIC numbers of the complainant and his wife. The respondent had not obtained the consent of the complainant and his wife for this disclosure of their personal data. The PDPC found that the respondent’s disclosure of personal data to Ms C was in breach of the PDPA.

19 In defence of his disclosure, the respondent took the view that he had acted in a “personal or domestic capacity” within the meaning of s 4(1)(a), “since his actions were unrelated to real estate matters”.¹⁸ However, the PDPC found that the respondent could not rely on s 4(1)(a) in this case because the personal data of the complainant and his wife had been initially collected by the respondent “in the course of his real estate agency work”, and not in a personal or domestic capacity.¹⁹ Even if he had later intended to act in a personal or domestic capacity in relation to the dispute between

15 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [14].

16 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [26].

17 [2017] PDP Digest 91.

18 *Re Chua Boon Yong Justin* [2017] PDP Digest 91 at [6].

19 *Re Chua Boon Yong Justin* [2017] PDP Digest 91 at [12].

the tenants, the respondent was not permitted to “take personal data that he had been provided with in his commercial capacity as a registered salesperson and disclose it in a personal or domestic capacity”.²⁰

20 In *Re Ang Rui Song*,²¹ the respondent was a financial consultant who had improperly disposed of his clients’ insurance policy documents. These documents contained sensitive personal data. Based on his representations, the respondent had simply put the documents into a plastic bag and placed them into a trash bin, and had not shredded the documents themselves. The PDPC found that the respondent had breached the PDPA by failing to take reasonable security arrangements to protect the personal data contained in the documents.

21 On the facts, the respondent in *Re Ang Rui Song* had ceased working as a financial consultant at the time of his disposal of the documents. However, adopting a similar line of reasoning to that taken in *Re Chua Boon Yong Justin*, the PDPC found that the respondent remained obliged to protect the personal data in the documents, even after he had ceased to be a financial consultant. Having obtained the personal data in the course of his business as a financial consultant, the respondent could not “unilaterally change the capacity” in which he possessed the personal data.²²

22 Thus, taken at their narrowest, *Re Chua Boon Yong Justin* and *Re Ang Rui Song* support the proposition that when an individual collects personal data in a capacity that is not personal or domestic, it is not open to that individual to later rely on s 4(1)(a) in relation to that personal data. To benefit from s 4(1)(a), an individual must consistently act in a personal or domestic capacity, and cannot have “switched” from acting in a business capacity.

III. Individual use of social media

23 The application of s 4(1)(a) is contextual: what counts as “acting in a personal or domestic capacity” depends on the factual context in which s 4(1)(a) is being employed. One difficult context which deserves some attention is the context of individual use of social media.

20 *Re Chua Boon Yong Justin* [2017] PDP Digest 91 at [13].

21 [2018] PDP Digest 236.

22 *Re Ang Rui Song* [2018] PDP Digest 236 at [11].

24 Social media enables individuals to access and publish personal data, on a global scale, at no financial cost to themselves. There are undeniable benefits to empowering individuals in this way. However, individuals do not always wield this power responsibly, and there is a legitimate concern that the publication of personal data on social media by private individuals may cause detriment to others.

A. The European Union approach

25 One possible response to this concern is to use data protection law to regulate individual use of social media. This appears to be the approach taken by the courts of the European Union (“EU”), which have taken a restrictive view of the personal and domestic exclusion in the European data protection legislation. This is discussed briefly below.

26 In *Bodil Lindqvist*²³ (“*Lindqvist*”), a catechist set up webpages for her parish, on which she uploaded information about herself as well as her parish colleagues. The Swedish Public Prosecutor prosecuted the catechist for infringing Swedish data protection law. The case was referred to the Court of Justice of the European Union (“CJEU”), and one of the questions referred was whether the conduct in question was exempted by the personal and domestic exclusion. In this regard, the court held that the personal and domestic exclusion did not apply to an individual who had loaded personal data on a webpage, as the personal data was published on the Internet such that it was made “accessible to an indefinite number of people”.²⁴

27 The *Lindqvist* approach was affirmed in the more recent case of *Sergejs Buivids*,²⁵ wherein the court held that the publication of a video by a private individual on YouTube could not fall within the scope of the personal and domestic exclusion, as it permitted “access to personal data to an indefinite number of people”.²⁶ In the court’s deliberation on the application of the

23 Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971; [2004] QB 1014.

24 Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971; [2004] QB 1014 at [47].

25 Case C-345/17 *Sergejs Buivids* [2019] ECLI:EU:C:2019:122; [2019] 1 WLR 4225.

26 Case C-345/17 *Sergejs Buivids* [2019] ECLI:EU:C:2019:122; [2019] 1 WLR 4225 at [43].

personal and domestic exclusion to the individual in question, no consideration was given to the fact that, unlike in *Lindqvist*, the individual had uploaded the video purely in a personal and private capacity.

28 Under the restrictive view of the personal and domestic exclusion taken by the CJEU, it is likely that any publicly viewable social media post containing personal data would fall outside the exclusion. Further, according to the Article 29 Data Protection Working Party, even in cases where the audience is limited to the user's contacts, the personal and domestic exclusion may not apply where a user has a "high number of third party contacts, some of whom he may not actually know".²⁷ Accordingly, such posts would in general be regulated by EU data protection law.

B. The Singapore approach

29 Singapore's approach to the issue, by contrast, appears to be less restrictive. A good hypothetical example of how s 4(1)(a) applies to individual use of social media may be found in the PDPC's guidelines, which is worth citing in full:²⁸

Diana, an employee of Organisation XYZ, attends Organisation XYZ's corporate social responsibility event. At the event, she meets her friend Dawn. During a break in the programme, they have a personal chat and catch up on each other's personal lives. During the chat, Diana takes a photograph of the two of them to update her friends of the encounter via social media. Diana then uploads the photograph and displays it on her personal social media page.

In this instance, Diana would likely be considered to be an individual acting in a personal or domestic capacity, and would not be required to comply with the Data Protection Provisions in respect of the photo-taking and subsequent disclosure of the photograph via her social media account.

Notwithstanding the above, the Data Protection Provisions may apply in other contexts where Diana is not acting in a personal or domestic capacity. For example, if the photograph is subsequently published for Organisation XYZ's publicity purposes (such as in Organisation XYZ's

27 Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking* (2009) at p 6. What constitutes a "high number" was left undefined.

28 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 4.7.

corporate brochures or website) instead of for Diana's personal purposes, the Data Protection Provisions are likely to apply to Organisation XYZ in respect of the collection, use and disclosure of the photograph. For example, Organisation XYZ will have to obtain Dawn's consent before publishing her photograph for Organisation XYZ's business purpose.

30 The approach taken in the above hypothetical example draws a clear distinction between social media posts made by individuals in a personal or domestic capacity, and social media posting in a business or work capacity. The focus here is, correctly, not on the publicity of the social media post but on the *capacity* in which the post was made. It is accordingly suggested that, in contrast with the EU position, an individual does not fall outside s 4(1)(a) merely because his social media post is publicly viewable.²⁹

31 It is argued that this approach does not result in under-regulation, because publication of personal data by individuals on social media platforms is subject to legal regulation by other laws in Singapore. The tort of defamation, which applies to individuals and legal entities alike, exists as a form of protection against defamatory statements made on social media platforms.³⁰ In addition, the Protection from Harassment Act³¹ has been amended to incorporate rules against the "disclosure of personal information to cause violence or harassment to others" (otherwise known as "doxxing"), thereby addressing the specific problem of online harassment via the disclosure of personal data online.³² In view of these legal protections against problematic forms of social media disclosures of personal data by private individuals, there does not appear to be a real necessity for the intervention of the PDPA in this regard.

29 This is arguably also consistent with the decision in *Re Grabcar Pte Ltd* [2020] PDP Digest 252: see especially [3(a)].

30 See, for example, *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] 2 SLR 751 where the plaintiffs sued for defamation in respect of the defendants' Facebook posts.

31 Cap 256A, 2015 Rev Ed.

32 Protection from Harassment Act (Cap 256A, 2015 Rev Ed) ss 3(1)(c) and 5(1A). See *Parliamentary Debates, Official Report* (7 May 2019), vol 94 (Edwin Tong Chun Fai, Senior Minister of State for Law, for the Minister of Law).

IV. Conclusion

32 As a personal and domestic exclusion, s 4(1)(a) is a significant carve-out from the scope of the PDPA. It is therefore important that the boundaries of s 4(1)(a) be well defined, such that it serves as a clear guide to conduct for individuals who may be dealing with personal data. To that end, this article has sought to explain the application of s 4(1)(a).

FIRST DO NO HARM: PROTECTING PATIENT DATA IN THE MODERN AGE*

Benjamin GAW†

*LLB (Hons) (National University of Singapore),
Specialist Diploma in Molecular Biotechnology (Ngee Ann Polytechnic);
Solicitor (England & Wales)*

Charis SEOW‡

LLB (Hons) (National University of Singapore)

I. Introduction

1 The past two years have been a whirlwind of activity in relation to data incidents in the healthcare sector. Following the high-profile cyberattack on the SingHealth patient database system in June 2018 where over 1.5 million patient records were accessed and copied, and the subsequent record-setting financial penalty that was imposed on SingHealth and its IT vendor by the Personal Data Protection Commission (“PDPC”) in 2019,¹ were a series of data incidents that affected several healthcare institutions in Singapore.

2 These data incidents included the discovery of the theft and illegal disclosure of the confidential HIV registry containing the personal data of 14,200 individuals in January 2019;² the mishandling of more than 800,000 registered blood donors’ personal information by Secur Group Solutions, an IT vendor of the Health Sciences Authority, which resulted in

* 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.

† Director, Corporate and Mergers & Acquisitions Practice Groups and Head, Healthcare & Life Sciences (Corporate & Regulatory), Drew & Napier LLC.

‡ Associate Director, Drew & Napier LLC.

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

2 Chang Ai-Lien, “Data of 14,200 People with HIV Leaked Online by US Fraudster who was Deported from Singapore” *The Straits Times* (28 January 2019).

a data leak in March 2019;³ and a data leak of 4,297 individuals' personal data after the Singapore Red Cross website was hacked on 8 May 2019.⁴ (The authors are not aware if the PDPC has investigated or intends to investigate the aforementioned organisations in question, although it is likely to do so.)

3 In addition, two healthcare institutions were the subject of enforcement action by the PDPC in 2019. In the case of Tan Tock Seng Hospital Pte Ltd⁵ ("TTSH"), the PDPC found that 85 notification letters meant for patients had been sent to the wrong address. With respect to the National Healthcare Group Pte Ltd⁶ ("NHG"), the PDPC found that a list containing the personal data of 129 partner doctors and several members of the public were publicly accessible online. While the PDPC only issued a warning to TTSH, NHG was found to be in breach of s 24 of the Personal Data Protection Act 2012⁷ ("PDPA") and was directed by the PDPC to pay a financial penalty of \$6,000.

4 The year 2019 also saw three highly-publicised Singapore Medical Council ("SMC") cases involving issues of medical confidentiality. Two of the cases involved doctors accessing patient databases without authorisation,⁸ while the third case involved a doctor disclosing patient data to a caller without verifying the identity of the caller.⁹

3 Felicia Choo, "Personal Information of over 800,000 Blood Donors was Accessible Online for 2 Months: HSA" *The Straits Times* (15 March 2019).

4 Goh Yan Han, "Singapore Red Cross Website Hacked, Details of Almost 4,300 Potential Blood Donors Leaked" *The Straits Times* (16 May 2019).

5 *Re Tan Tock Seng Hospital Pte Ltd* [2020] PDP Digest 550.

6 *Re National Healthcare Group Pte Ltd* [2020] PDP Digest 517.

7 Act 26 of 2012.

8 *Singapore Medical Council v Dr Leo Kah Woon* [2018] SMC DT 12; *Singapore Medical Council v Dr Ler Teck Siang* (Interim Orders Committee decision) (7 March 2019).

9 See *Singapore Medical Council v Dr Soo Shuenn Chiang* [2018] SMC DT 11 and *Singapore Medical Council v Soo Shuenn Chiang* [2019] SGHC 250. On appeal, the High Court, in setting aside Dr Soo's conviction, found that he had taken reasonable steps to ensure that the patient's medical information in the memorandum was not accessible to unauthorised persons, and that he had discharged his duty to maintain the patient's confidentiality.

5 In the wake of these data incidents in the healthcare sector, the authors are prompted to ask questions about the robustness of the legal protection for patient data. In this article, the following two questions will be discussed: (a) why are health-related organisations and institutions so vulnerable to attacks? and (b) how do the PDPA and current healthcare legislation protect patient data?

II. Why are health-related organisations and institutions so vulnerable to attacks?

A. *Patient data is a valuable target for hackers and criminals*

6 Beyond the obvious fact that health-related organisations and healthcare institutions are attractive targets because of the large volumes of patient data that they collect and store as part of their operations and processes, one reason why such organisations and institutions are seemingly so vulnerable to attacks may be due to the nature of patient data.

7 Patient data is inherently more valuable than other types of personal data, and, consequently, it is a prime target for hackers and criminals. A typical medical record may contain a range of information such as an individual's biographical information, medical history, diagnosis, prescriptions, billing information, insurance policy details, *etc.* Given this wealth of information, an individual's medical information can be several times more than valuable than credit card data on the black market. Stolen patient data can also be used by criminals to create fake identities in order to purchase expensive prescription drugs or medical equipment, or to file false insurance claims.¹⁰

8 The value of patient data to hackers and criminals is enhanced by the fact that patient data, in most scenarios, cannot be changed. In a typical data breach scenario, an individual can easily change his passwords or call his bank or credit card company to cancel his credit card. However, if his medical records were stolen, the individual cannot simply call the hospital or clinic to change his blood type, diagnosis or test results. Thus, the life span of patient data is longer compared to other types of records, and,

10 Caroline Humer & Jim Finkle, "Your Medical Record is Worth More to Hackers Than Your Credit Card" *Reuters* (25 September 2014).

consequently, the effects of unauthorised disclosure are more harmful and long-lasting.

B. Rapid expansion of new uses of patient data

9 Aside from its value to hackers and criminals, patient data also has immense value to legitimate organisations. During the first half of 2019, investments in health-related artificial intelligence (“AI”) topped US\$1.4bn.¹¹ The uses of patient data have rapidly expanded from the traditional purposes of teaching and research by hospitals, scientific centres and academic institutions, to the development of new drugs, medical devices and treatment by established pharmaceutical companies, to new commercial uses by medical technology (“MedTech”) companies.

10 These new commercial uses, which rely heavily on patient data or the analysis derived from health data, are vast and varied, ranging from the development of software for robot-assisted surgery; AI-driven advancements in clinical diagnostic support including natural language processing and diagnostic imaging; telemedicine applications offering virtual consultations with doctors and pharmacists, homecare services and house calls (*eg*, Doctor Anywhere, WhiteCoat, MyDoc, Speedoc, MaNaDr, HiDoc, Jaga-Me); innovations in the field of digital dentistry and orthodontics; to wearable technology, fitness trackers and “smart” health devices. In many instances, the collection of patient data by MedTech organisations is essential in order to provide the individual with personalised care and customised services.

11 In recognition of the potential benefits of telemedicine, defined as the “systematic provision of healthcare services over physically separate environments via Information and Communications Technology”,¹² the Ministry of Health (“MOH”) has published the *National Telemedicine Guidelines* to provide guidance on best practices in telemedicine interactions (including tele-collaboration, tele-treatment, tele-monitoring and tele-support) and ensure a holistic approach to the delivery of telemedicine services in Singapore.

11 CB Insights, “Global Healthcare Report Q2 2019” <<https://www.cbinsights.com/research/report/healthcare-trends-q2-2019/>> (accessed 30 January 2020).

12 Ministry of Health, “National Telemedicine Guidelines for Singapore” (30 January 2015).

12 Although these new commercial uses of patient data undoubtedly bring about health benefits to the individual and market value and profits to organisations, they also increase the risk of potential data incidents as an increasing number of MedTech start-ups and third-party developers are allowed access to patient data and to use patient data for novel purposes. If these MedTech start-ups and third-party developers do not put in place appropriate security measures to protect the patient data in their possession or control, the patient data will be at risk of unauthorised access and disclosure.

III. How do the Personal Data Protection Act 2012 and current healthcare legislation protect patient data?

A. Protection for patient data afforded by the Personal Data Protection Act 2012

13 The PDPA is a baseline data protection legislation which applies to all organisations that collect, use and disclose personal data, including patient data. Generally, the introduction of the PDPA has brought many benefits to the individual patient in the form of stronger protections for his personal data. For example, organisations are required to make reasonable security arrangements to protect the patient data in their possession or under their control.¹³ Patients also have increased autonomy and control over their data, *eg*, the right to withdraw consent, and the right to access and correct one's personal data (though these rights are not unqualified).

14 The PDPC, together with the MOH, also developed the *Advisory Guidelines for the Healthcare Sector*,¹⁴ to address sector-specific circumstances faced by the healthcare sector in complying with the PDPA. This includes the collection of patient data from patients seeking medical care; disclosing patient data in referral cases; collecting patient data to respond to an emergency; using patient data for research purposes; engaging third-party service providers to process patient data; responding to access and correction requests; and the retention of patient files and records, *etc*.

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

14 Revised 28 March 2017.

15 While there is no formal distinction in the PDPA for different categories of personal data, the PDPC has identified certain types of data to be more sensitive in nature, including patient data.¹⁵ As a general rule, where the personal data is regarded as more confidential and where the adverse impact on the individuals is significantly greater if such data were inadvertently accessed, as is the case with patient data, tighter security arrangements should be employed.¹⁶

16 The PDPC has also stated in several enforcement decisions that a higher standard of protection is required for sensitive personal data.¹⁷ In the case of *Re Singapore Health Services Pte Ltd*,¹⁸ the PDPC determined that the patient data in question, which contained clinical episode information, clinical documentation, patient diagnosis and health issues and dispensed medication records, was considered to be “highly sensitive and confidential personal data”. The PDPC acknowledged the “potential embarrassment that a patient may suffer if such sensitive information about the patient and the patient’s health concerns were made known to all and sundry”,¹⁹ and concluded that it was critical for organisations to protect the security and confidentiality of such medical records.

17 The baseline protection for personal data afforded by the PDPA is a welcome improvement, as is the PDPC’s requirement that organisations provide stronger safeguards when dealing with sensitive personal data.

15 Other types of sensitive personal data include national identification numbers; financial data, insurance data; an individual’s history involving drug use and infidelity; the personal data of minors; and sensitive medical conditions. See *Re Aviva Ltd* [2018] PDP Digest 245; *Re Credit Counselling Singapore* [2018] PDP Digest 295; *Re Singapore Taekwondo Federation* [2019] PDP Digest 247; *Re AIA Singapore Private Limited* [2020] PDP Digest 298; *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188.

16 Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised 28 March 2017) at para 4.2.

17 Personal Data Protection Commission, *Advisory Guidelines for the Healthcare Sector* (revised 28 March 2017) at para 4.2. See also Lanx Goh & Nadia Yeo, “Sensitive Personal Data in the Singapore Context?” [2019] PDP Digest 37 and Benjamin Wong YongQuan, “Protection of Sensitive Data” [2018] PDP Digest 19.

18 [2019] PDP Digest 376.

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

While the fact that the PDPC does not intend to create a two-tier definition of personal data, and simultaneously wishes to reserve for itself some flexibility in the interpretation of what it considers to be “stronger safeguards”, is appreciated, given that organisations face severe consequences for data incidents involving patient data, it is anticipated that there may be further clarity from the PDPC in the near future on what constitutes such “stronger safeguards” either in the form of guidelines or findings in grounds of decision.

B. Protection for patient data afforded by healthcare legislation

18 There is no standalone healthcare legislation in Singapore which regulates the collection, use and disclosure of patient data. Instead, there is a patchwork of laws which contain provisions on the security and confidentiality of patient data. With the advent of the PDPA, Parliament has clarified that the healthcare sector will continue to be regulated by the existing healthcare laws, and doctors and healthcare institutions “will continue to be subject to existing patient confidentiality requirements”.²⁰ The PDPA will apply concurrently and, in cases of inconsistency between the provisions of the PDPA and provisions of other written laws, the latter will prevail.²¹

(1) Protection Obligation and patient confidentiality

19 The safeguarding of an individual’s personal data is the keystone of many data protection laws, including the PDPA. Similarly, the maintenance of the privacy of patients has been described as the cornerstone of the ethics of the medical profession.²²

20 All organisations (including data intermediaries) that are subject to the PDPA must comply with the Protection Obligation²³ in respect of the personal data that they have in their possession or control. As there is no

20 *Parliamentary Debates, Official Report* (16 September 2013), vol 90 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communication and the Arts).

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

22 *Singapore Medical Council Disciplinary Committee Inquiry for Dr Singh Tregon Randhawa* (29 November 2011) at [8].

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

one-size-fits-all solution for each organisation, the security measures adopted may differ depending on factors such as the nature of the personal data, the form in which it is collected, and the possible impact on the individual if an unauthorised person obtained, modified or disposed of the personal data. A higher level of security would be expected for more confidential types of data.

21 In comparison, the security measures relating to patient confidentiality seem more dependent on the identity of the healthcare stakeholder (doctors, nurses, allied health professionals,²⁴ healthcare institutions, *etc*) in question and less dependent on the factors surrounding the collection, use and disclosure of the patient data. While healthcare stakeholders have a general duty to ensure patient confidentiality, the standards of such protection are governed by different legislation and frameworks.

22 For instance, medical practitioners are bound by rules of professional and ethical conduct, which include medical confidentiality obligations, under the SMC's *Ethical Code and Ethical Guidelines*²⁵ ("SMC ECEG"), whereas licensees under the Private Hospitals and Medical Clinics Act²⁶ ("PHMCA") must comply with the provisions relating to the confidentiality of medical records relating to the condition, treatment or diagnosis of any person.²⁷ Researchers subject to the Human Biomedical Research Act 2015²⁸ have a duty to protect individually-identifiable information and human biological material against accidental or unlawful loss, modification or destruction, or unauthorised access, disclosure, copying, use or modification.²⁹

23 From a historical perspective, data protection and privacy laws have their roots in the aftermath of the Second World War and the 1948

24 7The allied health professions that are regulated under the Allied Health Professions Act (Cap 6B, 2013 Rev Ed) are occupational therapists, physiotherapists, speech-language therapists, diagnostic radiographers and radiation therapists.

25 Section C7 of the Singapore Medical Council, *Ethical Code and Ethical Guidelines* (2016 Ed).

26 Cap 248, 1999 Rev Ed.

27 Private Hospitals and Medical Clinics Act (Cap 248, 1999 Rev Ed) s 13.

28 Act 29 of 2015.

29 Human Biomedical Research Act 2015 (Act 29 of 2015) s 27.

Universal Declaration of Human Rights (whose drafters were influenced by the US Bill of Rights), whereas the concept of patient confidentiality pre-dates the modern era and can trace its origins to the Hippocratic Oath which was written in the fifth century.³⁰ Modern-day medical practitioners are still required to keep confidential any information provided to them by patients in the context of clinical care, subject to exceptions.³¹

24 One example of a breach of medical confidentiality is a doctor's unauthorised access of patient data when he is not involved in any aspect of the patient's care.³² Highlighted here is the case of *Singapore Medical Council v Dr Leo Kah Woon*,³³ in which a doctor accessed a hospital's clinical manager system, which contained electronic medical records of patients, to search for the contact details of the spouse of his wife's alleged lover. Dr Leo was charged with and convicted of two offences in the State Courts under the Computer Misuse Act³⁴ for which he pleaded guilty and was fined a total of \$13,000. The criminal charges made Dr Leo liable for punishment under s 53(1)(b) of the Medical Registration Act³⁵ ("MRA").

25 The disciplinary tribunal ("DT"), in censuring Dr Leo and suspending him for three months, considered that a mere fine would be insufficient to redress the breach of trust and deter likeminded doctors from "abusing the privilege and accessing such a database for purely his or her own personal reasons or benefit".³⁶ The DT also dismissed the argument

30 Ian E Thompson, "The Nature of Confidentiality" (1979) 5(2) *Journal of Medical Ethics* 57. The provision on confidentiality reads as follows: "And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."

31 Section C7(5) of the Singapore Medical Council, *Ethical Code and Ethical Guidelines* (2016 Ed). The confidential information of patients may only be disclosed without consent if there are sound justifications, for example where mandated by law; if it is necessary to protect patients or other third parties from harm; when the involvement of parents and legal guardians is beneficial to minors; or where such disclosure is in the patient's best interests.

32 Section C7(3) of the Singapore Medical Council, *Ethical Code and Ethical Guidelines* (2016 Ed).

33 [2018] SMC DT 12.

34 Cap 50A, 2007 Rev Ed.

35 Cap 174, 2014 Rev Ed.

36 *Singapore Medical Council v Dr Leo Kah Woon* [2018] SMC DT 12 at [71].

that Dr Leo's actions arose out of a private domestic matter and stated that the public expects doctors "to keep medical records confidential, be they personal information or details of medical treatment".³⁷

26 While this case was not the subject of enforcement action by the PDPC, the authors speculate that if the PDPC had opened an investigation into the case, it would be likely that the PDPC would first consider the hospital, as the organisation in possession and control of the patient data in the clinical manager system, to be the party responsible for the protection of such data. Under the PDPA, liability is imposed on employers for acts of their employees. Pursuant to s 53(1), the hospital would *prima facie* be responsible for the data incident caused by its employee's (*ie*, Dr Leo's) actions, regardless of whether his actions were done with the hospital's knowledge or approval.

27 However, on the facts, it would be open for the hospital to raise a defence under s 53(2) of the PDPA and prove that it took such steps as were practicable to prevent Dr Leo from engaging in such acts in the course of his employment. To the authors' knowledge, this defence has not been raised before in any of the published enforcement decisions. Moreover, it may also be open for the hospital to argue that the doctor was not acting in the course of his employment and therefore should not be able to rely the employee exemption under s 4(1)(b) of the PDPA.³⁸

28 The above analysis is based on the authors' understanding that Dr Leo was an employee of the hospital at the material time. Notwithstanding this, the authors are aware that there are other scenarios where the doctor in question is not an employee but instead an independent contractor engaged by the hospital or sole proprietor of a clinic within the hospital. In these alternative scenarios, it is possible that the PDPC would impose data protection obligations on such doctors as separate "organisations" under the PDPA.

37 Singapore Medical Council v Dr Leo Kah Woon [2018] SMCDDT 12 at [69].

38 Section 4(1)(b) of the Personal Data Protection Act (Act 26 of 2012) states that Pts III–VI shall not impose any obligation on "any employee acting in the course of his employment with an organisation".

(2) *Protection Obligation and medical records*

29 Turning to the issue of medical records, the authors first consider the National Electronic Health Record (“NEHR”) system,³⁹ which builds upon the pre-existing Electronic Medical Records (“EMR”) system within public hospitals. Information that is entered into local EMR systems (which includes detailed transactional records of patients that allow healthcare workers to enter clinical observations or assessments, order medication, make electronic orders for tests, and review results and radiological images) is automatically extracted and sent to the NEHR. In terms of security measures, public healthcare institutions contributing to and accessing the NEHR are required to comply with nationwide cybersecurity standards to protect patient data, which include using a two-factor authentication system to access patient records.

30 There are further obligations imposed on healthcare stakeholders in relation to the protection and maintenance of proper medical records. Pursuant to reg 12 of the Private Hospitals and Medical Clinics Regulations⁴⁰ (“PHMCR”), licensees of private hospitals, medical clinics, clinical laboratories and healthcare establishments are required to keep and maintain proper medical records and record the particulars of each patient. Licensees are also required to, *inter alia*, implement adequate safeguards (whether administrative, technical or physical) to protect the medical records against accidental or unlawful loss, modification or destruction, or unauthorised access, disclosure, copying, use or modification.⁴¹

31 Although the wording used in reg 12 of the PHMCR is remarkably similar to the Protection Obligation in the PDPA, the potential penalties under each framework are distinct. A person who contravenes a regulation in the PHMCR shall be guilty of an offence and liable on conviction to a fine not exceeding \$2,000 or to imprisonment for a term not exceeding

39 There is currently no specific legislation governing the National Electronic Health Record (“NEHR”). The coming Healthcare Services Act 2020 (Bill No 37/2019) was intended to include provisions mandating NEHR contributions; however, these provisions were removed when the plans for mandatory NEHR contributions were deferred.

40 Cap 248, Rg 1, 2002 Rev Ed.

41 Private Hospitals and Medical Clinics Regulations (Cap 248, Rg 1, 2002 Rev Ed) reg 12(1A)(b).

12 months or to both.⁴² In contrast, the PDPC is empowered to issue an organisation that is in breach of the Protection Obligation directions to destroy or stop collecting, using or disclosing the personal data, or to pay a financial penalty not exceeding \$1m.⁴³

32 However, it should be highlighted that the PHMCA (and the PHMCR) will soon be repealed and replaced by the Healthcare Services Act 2020⁴⁴ (“HCSA”), which has been passed by Parliament on 6 January 2020. The HCSA, which is intended to regulate and license healthcare services, introduces higher penalties for the failure to keep and maintain healthcare records. Although the wording in s 27(2) of the proposed new legislation closely mirrors reg 12(1A)(b) of the PHMCR, the penalty for a contravention of the former is a fine not exceeding \$20,000 or imprisonment for a term not exceeding 12 months or both.⁴⁵

33 As another example, the Human Biomedical Research (Tissue Banking) Regulations 2019,⁴⁶ which regulate tissue banking activity and the handling of human tissue for use in research, impose obligations on every tissue bank to establish a system which puts in place reasonable measures as may be necessary to protect the confidentiality of information relating to the donor of each tissue under the supervision and control of the tissue bank and to maintain the donor’s privacy.⁴⁷ The penalty for tissue banks that do not comply is a fine not exceeding \$10,000, or (in the case of an individual) a fine not exceeding \$10,000, or imprisonment for a term not exceeding 12 months or both.⁴⁸

34 There are also ethical obligations imposed on doctors in relation to the maintenance of proper medical records. Under the SMC ECEG, doctors are required to keep medical records safely and securely and ensure that the records are not at risk of unauthorised access and breach of medical

42 Private Hospitals and Medical Clinics Regulations (Cap 248, Rg 1, 2002 Rev Ed) reg 60.

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

44 Healthcare Services Bill (No 37/2019).

45 Healthcare Services Bill (No 37/2019) s 27(5).

46 S 702/2019.

47 Human Biomedical Research (Tissue Banking) Regulations 2019 (S 702/2019) reg 16(1).

48 Human Biomedical Research (Tissue Banking) Regulations 2019 (S 702/2019) reg 16(2).

confidentiality. If the doctor is not in control of the medical record system, the doctor has a duty to use the system responsibly and abide by all the security protocols in place.⁴⁹ Although there are no penalties in the SMC ECEG, a doctor's failure to protect medical records may open him to a charge of professional misconduct under s 53(1)(d) of the MRA, under which the maximum penalty that may be imposed is \$100,000.⁵⁰

35 In view of the serious penalties for the failure to protect medical records, there is a need to determine what constitutes reasonable security arrangements in the context of protecting patient data. At this juncture, the focus turns to another industry which handles large volumes of sensitive data: the financial sector. The Monetary Authority of Singapore has developed the *Guidelines on Risk Management Practices – Technology Risk*⁵¹ which set out, *inter alia*, best practices to guide all financial institutions in the deployment of strong IT controls to protect customer data from unauthorised access or disclosure. Borrowing from this approach, one suggestion would be for MOH, in collaboration with the PDPC, to develop industry-wide guidelines on how all healthcare stakeholders should treat and protect patient data, and what would be considered reasonable security arrangements that are appropriate in the circumstances.

IV. Concluding thoughts

36 As illustrated in the examples above, the field of healthcare services is varied and involves multiple stakeholders. One observation is that there may be scenarios in which some stakeholders (*eg*, medical practitioners and licensed healthcare institutions) have additional obligations in respect of the protection of patient data as compared to other organisations (*eg*, data analytics companies and IT service providers). This stems from the fact that the healthcare sector has traditionally regulated different stakeholders through separate legislation and frameworks.

37 Another observation is that there seems to be agreement across the board that patient data is more sensitive in nature and warrants a higher

49 Section B3(8) of the Singapore Medical Council, *Ethical Code and Ethical Guidelines* (2016 Ed).

50 Medical Registration Act (Cap 174, 2014 Rev Ed) s 53(2)(e).

51 Published 1 June 2013.

level of safeguards. However, there does not seem to be a consensus as to what constitutes this higher standard of protection. Whilst the existing standards of protection for patient data may be adequate for now, it is anticipated that this lack of consensus may cause problems in the future, given the growing value of patient data and the rapid expansion of new uses of patient data (*eg*, in telemedicine, MedTech and AI).

38 Undoubtedly, there is a strong need for a robust regime of protection for patient data. Taking the above observations into account, the authors believe that there is room to develop a more streamlined approach to safeguarding patient data, either through the crafting of industry-wide guidelines which articulate how relevant healthcare stakeholders should treat and protect sensitive patient data, or the creation of a dedicated personal health information law to replace the existing piecemeal healthcare legislation.

CIVIL PROCEEDINGS UNDER THE PERSONAL DATA PROTECTION ACT 2012*

Alexander YAP Wei-Ming[†]

MA (Oxon);

Advocate and Solicitor (Singapore)

TAY Yong Seng[‡]

MA BCL (Oxon);

Advocate and Solicitor (Singapore)

ANG Ann Liang[§]

LLB (University College London);

Advocate and Solicitor (Singapore)

Brenda SOH[¶]

LLB (London School of Economics and Political Science);

Advocate and Solicitor (Singapore)

I. Introduction

1 An important aspect of data protection compliance, from a practical perspective, relates to how data protection laws are, or may be, enforced. In Singapore, the key legislation governing data protection is the Personal Data Protection Act 2012¹ (“PDPA”). Organisations and individuals may find knowledge of PDPA enforcement trends and practices to be helpful because it allows them to more accurately evaluate risks from acts or omissions which may constitute a breach of the PDPA. Such knowledge may also assist them in determining how to seek redress, in circumstances

* Any views expressed in this article are the authors’ personal views only and should not be taken to represent the views of Allen & Gledhill LLP. All errors remain the authors’ own.

† Partner, Allen & Gledhill LLP.

‡ Partner, Allen & Gledhill LLP.

§ Senior Associate, Allen & Gledhill LLP.

¶ Senior Associate, Allen & Gledhill LLP.

1 Act 26 of 2012.

where a third party may have breached the data protection requirements of the PDPA.

II. Enforcement of the Personal Data Protection Act 2012

A. Enforcement by the Personal Data Protection Commission

2 Enforcement of the PDPA in Singapore is most often carried out by the Personal Data Protection Commission (“PDPC”), the local data protection watchdog. This conclusion has been reached simply because there have been numerous data protection enforcement cases published by the PDPC² as compared to a single published judgment of the Singapore courts.³

3 The PDPC is the Infocomm Media Development Authority,⁴ a statutory board⁵ of the Singapore Government under the Ministry of Communications and Information.⁶ It has broad powers to enforce the PDPA, conferred by the PDPA and its subsidiary legislation. These include powers to review an organisation’s reply to a request made by an individual under s 21 or 22 of the PDPA,⁷ powers relating to investigation in respect

2 The Personal Data Protection Commission maintains a website upon which it publishes cases, under the heading “All Commission’s Decisions” <<https://www.pdpc.gov.sg/All-Commissions-Decisions?keyword=&industry=all&nature=all&decision=all&penalty=all&page=1>> (accessed 18 July 2020). Based on an internally created compilation with decisions up to 19 March 2020, there have been 138 decisions published on such website, but any error or omission is regretted, and note that this number does not include “case summaries” published by the Commission in the *Personal Data Protection Digest*.

3 As at 18 July 2020, the authors are only aware of one published judgment of the Singapore courts where relief was sought pursuant to s 32 of the Personal Data Protection Act 2012 (Act 26 of 2012), *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207. This case, and the accuracy of this measure, is discussed later in this article.

4 Personal Data Protection Act 2012 (Act 26 of 2012) s 5(1).

5 Established under s 3 of the Info-Communications Media Development Authority Act 2016 (Act 22 of 2016).

6 MCI Agencies <<https://www.mci.gov.sg/agencies>> (accessed 18 July 2020).

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

of contraventions of the PDPA⁸ and powers to issue directions to secure an organisation's compliance with the data protection provisions of the PDPA.⁹ The PDPC has also made statements on particular mechanisms for enforcement which it has adopted, including an "undertakings" process¹⁰ and a procedure for expedited breach decisions.¹¹ The PDPC has, in the authors' experience, exercised all of the powers described above.

4 While the PDPC has been said to adopt "a complaints-based approach to enforcement",¹² the PDPC also has jurisdiction to initiate investigations *suo moto* (on its own motion)¹³ and has carried out investigations as a result of self-reporting of actual or potential data protection breaches. Of the data protection cases published by the PDPC on its website¹⁴ up to 19 March 2020, of "decisions relating to organisations that are found to have contravened the data protection provisions under the Personal Data Protection Act", approximately¹⁵ 70% of the decisions were stated (or were otherwise suggested) as having arisen from complaints or reports to the PDPC, including by members of the public, third-party organisations or a different government authority, 23% of the decisions were stated as having arisen from self-reporting by

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 50.

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

10 Personal Data Protection Commission, *Guide on Active Enforcement* (published 22 May 2019).

11 Personal Data Protection Commission, *Guide on Active Enforcement* (published 22 May 2019).

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

13 Personal Data Protection Act 2012 (Act 26 of 2012) ss 6 and 29.

14 Personal Data Protection Commission, "All Commission's Decisions" <<https://www.pdpc.gov.sg/All-Commissions-Decisions?keyword=&industry=all&nature=all&decision=all&penalty=all&page=1>> (accessed 18 July 2020).

15 These percentages are based on an internally created compilation. This compilation does not take into account "case summaries" published by the Personal Data Protection Commission in the *Personal Data Protection Digest*, and as categorisation requires an exercise of judgment, the percentages may not be accurate and at most should be treated as being somewhat indicative.

organisations, and based on the foregoing, up to 7%¹⁶ may have arisen due to the PDPC acting *suo moto*, or other than due to third-party complaints or reports and self-reporting.¹⁷

B. Civil proceedings under section 32 of the Personal Data Protection Act 2012

5 Section 32 of the PDPA provides that any person who has suffered loss or damage directly as a result of contravention of any provision in the data protection provisions of the PDPA has a right of action for relief in civil proceedings in the Singapore courts against the breaching organisation. Such a right of private action is not unusual from a data protection perspective, with similar rights of private action having been included in new US consumer privacy legislation, and in European data protection legislation.¹⁸

6 As discussed above, enforcement of the PDPA in Singapore is most often carried out by the PDPC in the exercise of its powers under the PDPA. However, the measure used to reach this conclusion, the number of published judgments of the Singapore courts, may not be entirely determinative. In the authors' experience, it is not unusual for an individual or organisation who has suffered loss or damage due to a breach of the data protection provisions of the PDPA to reach some type of resolution with the breaching organisation¹⁹ through direct communication with the breaching organisation, without any PDPC involvement. This could occur where the aggrieved individuals or organisations themselves approach the breaching organisation (with or without knowledge of the right of private

16 This percentage is the most uncertain. This categorisation was created to reflect all decisions where the reason the investigation began was unclear or was stated as being due to a news report. The authors have sought to exclude from this percentage all instances where the decision indicated the existence of one or more complainants, or of any self-reporting.

17 Note that the possibility cannot be excluded that in this categorisation of Personal Data Protection Commission decisions the existence of a complainant or of self-reporting was simply not mentioned.

18 In particular in the Consumer Privacy Act of the State of California, US and in the General Data Protection Regulation ((EU) 2016/679; entry into force 25 May 2018).

19 If, in fact, the breaching organisation is identifiable and has been identified.

action in s 32 of the PDPA) or where such aggrieved individuals or organisations seek the assistance of legal counsel to “ghost write” letters, or issue letters of demand. In the authors’ experience, it is not unusual for such direct communications to result in a final resolution of the matter at hand, although occasionally there may also be a prior or subsequent complaint to the PDPC.

7 Having said that, it is likely still true that enforcement of the PDPA in Singapore is most often carried out by the PDPC, due to the vast difference in numbers – 138²⁰ published decisions of the PDPC *versus* one published judgment of the Singapore courts, and also because not every PDPC investigation results in a decision being published, for example because the PDPC became convinced in the course of that investigation that there was no breach of the PDPA, or otherwise decided to discontinue an investigation.

8 As of the date this article was first prepared,²¹ the only published judgment of the Singapore courts where relief was sought pursuant to s 32 of the PDPA is the case of *IP Investment Management Pte Ltd v Alex Bellingham*²² (“*IPvA*”).²³

20 This number is based on an internally created compilation with decisions up to 19 March 2020, and any error or omission is regretted. Note that “case summaries” published by the Personal Data Protection Commission in the *Personal Data Protection Digest* are not included in this number.

21 January 2020. A check as at 18 July 2020 using the “Reference Trace” function of the Lawnet website <<https://www.lawnet.sg>> operated by the Singapore Academy of Law indicates that as of that date, *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 continues to be the only published judgment of the Singapore courts where relief was sought pursuant to s 32 of the Personal Data Protection Act 2012 (Act 26 of 2012).

22 [2019] SGDC 207.

23 Several authors of this article acted as counsel for the plaintiffs in *IP Investment Management Pte Ltd v Alex Bellingham*. All comments in this article on this case are made in view of only the published judgment, *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207. The High Court allowed the appeal against the decision on 11 September 2020, but on a separate point. The issues discussed in this article do not pertain to the issues raised on appeal and, and the authors do not purport to express any opinion on the appeal in this article or any of the issues raised in the appeal.

III. Key elements required for section 32 to be relevant

9 Briefly, the following are the key elements that a plaintiff seeking to bring an action under s 32 of the PDPA should note.

A. *Locus standi*

10 When considering s 32 of the PDPA, it would be pertinent to know who has *locus standi* to bring an action under such provision. The PDPA simply provides that such right of private action is available to any “person who suffers loss or damage directly as a result of a contravention of any provision in Parts IV, V or VI by an organisation”. *IPvA* further clarified that the word “person” in the context of the PDPA should be interpreted to refer only to individuals whose personal data forms the subject of the alleged breach of the PDPA, and should not include corporate bodies (such as companies).²⁴

B. *Loss or damage*

11 A plaintiff exercising its right of private action under s 32 of the PDPA must also prove that the plaintiff has suffered loss or damage directly as a result of a contravention of any provision in Parts IV, V or VI of the PDPA by an organisation.²⁵ The PDPA does not expressly state the type of loss or damage suffered that may avail the plaintiff to such right of private action. Section 32 of the PDPA does provide that relief will be granted as long as it can be proved that such loss or damage has resulted directly from the breach in question.

24 While it is arguable that “person”, which is not defined in the Personal Data Protection Act 2012 (Act 26 of 2012) itself, may be interpreted to include corporate bodies based on the definition of “person” in the Interpretation Act (Cap 1, 2002 Rev Ed), the Singapore court in *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 chose not to take such an approach. This is further discussed later in this article.

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

C. Decision from Personal Data Protection Commission (if any) must be final

12 Additionally, pursuant to s 32(2) of the PDPA, no action may be brought under s 32(1) of the PDPA if the PDPC has made a decision under the PDPA in respect of the same contravention of the PDPA, until such time the decision has become final as a result of there being no further right of appeal. As such, it is crucial to plan in advance which “route” (civil proceedings or a complaint to the PDPC) would be most effective for securing the most favourable outcome, in time, taking into account any requirements the plaintiff may have, with this restriction in mind.

D. Relief available

13 The court hearing an action pursuant to s 32 of the PDPA may grant an injunction or declaration, damages and/or such other relief as it thinks fit.²⁶

IV. Significance and implications of *IPvA*: Clarifying the rationale behind the Personal Data Protection Act 2012 – whether section 32 extends to companies

14 *IPvA* sought to explain the rationale behind s 32 of the PDPA. In particular, one key issue discussed was whether companies were included within the scope of “person” as referred to in s 32.

A. Alignment with data protection laws of other jurisdictions

15 In *IPvA*, the Singapore court made it clear that s 32 of the PDPA ought to be interpreted in a manner consistent with one of the primary motivating factors underlying the promulgation of the PDPA, which is to align local data protection laws with those of other jurisdictions.²⁷ There was no evidence of any jurisdiction in which an entity, other than a data subject, was able to have recourse to a right of private action similar to that

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

27 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [93]–[97].

provided for under s 32 of the PDPA, for its own benefit.²⁸ The Singapore court in *IPvA* suggested that legislation from the UK and Hong Kong seemed to accord such a right of private action only to individual data subjects.²⁹

B. Means for individuals to seek compensation

16 The Singapore court in *IPvA* highlighted that during the Second Reading of the Personal Data Protection Bill 2012,³⁰ it was stated that the Bill “allows individuals to seek compensation for damages directly suffered from a breach of the data protection rules through private rights of action” without mention of any intention for such right to be conferred on companies or other non-individuals.

C. A “kind of crutch” which may “severely undermine” the aim of the Personal Data Protection Act 2012

17 The decision in *IPvA* adopted the view that s 32 should not be read in a way that would allow organisations to use it as a “substitute for contractual or other arrangements, which they might otherwise have been expected to put in place (for instance, pursuant to section 24 of the PDPA), to protect personal data in their possession”.³¹ The Singapore court in *IPvA* adopted the approach that the responsibilities of data collecting organisations under the PDPA in relation to data breaches are generally preventive in nature and that organisations’ fulfilment of such obligations should put them in the position to be able to take remedial steps to address any data breaches. For instance, the court referred to the PDPC decision of *Re Watami Food Service Singapore Pte Ltd*³² as an example of where an organisation was able to take the relevant remedial steps following a data

28 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [97].

29 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [99].

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

31 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [85].

32 [2019] PDP Digest 221.

breach because “independently of section 32 of the PDPA, it had already put in place arrangements which permitted it to do so”.³³ In *IPvA*, the court’s view was that the plaintiffs were seeking to use s 32 as a substitute for contractual or other obligations, and allowing organisations in such a position to avail themselves of s 32 would give entities a “kind of crutch”³⁴ to seek recourse via civil proceedings for losses, and “severely undermine”³⁵ the aim of the PDPA as legislation to safeguard individuals’ personal data against misuse by regulating the proper management of personal data.³⁶

D. Object of the Personal Data Protection Act 2012 to promote “prevention” of data breaches instead of to provide remedies in the event of data breaches

18 In *IPvA*, the plaintiffs argued that providing companies with a right of private action under s 32 of the PDPA would promote the PDPA’s statutory purpose of protecting personal data, and would therefore enhance Singapore’s status as a data hub.

19 The plaintiffs argued, amongst other things, that if s 32 were to be restricted only to the individual data subjects, then in an instance of, for example, wilful breaches of the PDPA caused by an errant former employee of a company, the only remedy left to the company would be to make a “passive request” to the errant employee for return or deletion of the personal data.³⁷ Such a “passive remedy” would be effective only if the errant former employee is willing to co-operate and return or delete the personal data. If the errant former employee is recalcitrant and refuses, then the company may not have any other legal recourse to compel the return and deletion of the personal data. In the circumstances, the plaintiffs argued

33 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [83].

34 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [86].

35 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [86].

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

37 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [75] and [76].

that the need for companies to have a right of private action under s 32 of the PDPA against errant former employees is plain.³⁸

20 However, notwithstanding the plaintiffs' arguments above, the court eventually held that companies should not be allowed to seek redress under s 32. The court held that the object of the PDPA was to promote "prevention" of data breaches, instead of remedies in the event of data breaches. In the circumstances, as the law presently stands, companies and organisations do not have a right of private action under s 32 of the PDPA. Companies would be well advised to, as much as possible, put in place as many preventive measures as possible, including the use of contractual obligations, to protect personal data.

V. "Privacy"-centric legal approach versus an "economic" approach

21 Restricting the right of private action under the PDPA to individuals is reflective of a more "privacy"-centric approach, such as in Europe where privacy legislation is largely driven by a strong focus on privacy as a fundamental human right.³⁹ That analysis starts from legal principles and contemplation of privacy from a legal standpoint.

22 Thinking outside the legal sphere, and taking a wider economic standpoint (rather than a purely legal one), one could perhaps contemplate a different economic approach by policymakers in a world where "data is king", or "data is the new oil".⁴⁰ Countries around the world are competing to become data hubs for increasingly data-driven industries, and Singapore is no different. Data protection law in Singapore has, since its inception, been driven by a pragmatic desire to enhance Singapore's competitiveness and strengthen its position as a trusted business hub.⁴¹ Singapore's

38 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [75] and [76].

39 Simon Chesterman, "After Privacy: The Rise of Facebook, The Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012" [2012] 2 *Singapore Journal of Legal Studies* 391.

40 For example, "The World's Most Valuable Resource is No Longer Oil, But Data" *The Economist* (6 May 2017).

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

inclination towards such an “*economic*” rather than “*privacy*”-centric legal approach is suggested by the lack of recognition of a general right to privacy in statutory or common law in Singapore⁴² and the PDPC’s decisions which appear to focus on “informational privacy” and how it should not be distorted to address privacy issues that it was not meant to address.⁴³

23 Extending the application of a private action such as the one under s 32 of the PDPA to companies could practically enhance a company’s right to collect, use and disclose personal data since this would give companies greater recourse in the event of loss or damage arising directly from a breach of the PDPA by a third party (hacker). This may encourage companies to deal directly with data-related operations within Singapore, in particular companies in industries where the collection, use and/or disclosure of personal data is crucial to their businesses (*eg*, technology companies, financial institutions, insurance companies, healthcare providers and other entities which collect significant amounts of personal data as part of their day-to-day business activities) or other companies whose business activities are highly dependent on third-party data storage or processing services such as cloud computing. The availability of civil proceedings as an avenue of protection from loss or damage arising from a third party’s breach of the PDPA may lower the risk of having to absorb such loss or damage themselves, or at least allow their insurers some measure of recovery.

24 This is especially true for two reasons. First, cybersecurity breaches are often treated as something which will occur “not if but when”.⁴⁴ In such a climate, especially where a hacker is identified, hackers may be deterred if a company (with superior means and deeper pockets than an individual) can take direct action against them on behalf of an affected individual. Such deterrent effect is not likely to be affected by whether or not the hacker has, or had, any contractual or other relationship with that company, and in any

42 *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334 at [21].

43 *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334 at [51].

44 For example: (a) *Cybersecurity: A View from the Boardroom* (Cisco, 2015) <https://www.cisco.com/c/dam/r/en/us/internet-of-everything-ioe/assets/files/Cybersecurity_A_View_from_the_Boardroom_HighRez.pdf> (accessed 18 July 2020); and (b) “Cyber Security Experts Like to Espouse the Cliche that It’s Not If, But When, an Organisation Will Be Hacked”: excerpt from “Consider ‘Hack Mindef’ Initiative to Suss Out Bugs” *The Straits Times* (7 March 2017).

case, the hacker would likely not have any relationship with the affected individual, just as he is not likely to have a prior relationship with the company. Second, while private actions taken out by companies for affected individuals could lead to higher legal costs for the company, it should be noted that global organisations already face heightened costs for data protection related litigation, for example, under the (relatively) new California Consumer Privacy Act of 2018 (“CCPA”).⁴⁵ One US firm recently hosted a continuing legal education seminar focused on the CCPA, with a synopsis which stated, rather alarmingly, “and that includes preparing for the inevitable onslaught of class action litigation that is coming”.⁴⁶ The statement seemed prescient. Within two months from the date that the CCPA came into force, there have been at least two class action lawsuits filed.⁴⁷

VI. Considerations relevant to potential future actions

25 The Singapore courts have confirmed in *IPvA* that redress under s 32 is unavailable to companies. Companies would now be left to rely on other methods to obtain relief for losses suffered, and in doing so would have to consider a number of factors to determine the most appropriate course of action. Companies, not being individual data subjects, would simply have

45 The authors believe that any natural person with California residency has a right of action under the California Consumer Privacy Act of 2018 if their non-encrypted and non-redacted personal information has been exposed due to a business’s failure to maintain reasonable and appropriate security safeguards, under §1798.150 of Title 1.81.5. <https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.150> (accessed 18 July 2020).

46 “The CCPA Is Here – Are You Litigation Ready” *Hunton Andrews Kurth* (2 April 2020).

47 Ring LCC: Elizabeth Casale, James Shreve & Luke Sosnicki “Class-action Case against Ring may Test CCPA’s Private Right of Action” *Thomson Coburn LLP* (24 February 2020); Hanna Andersson LLC: Kyle Brasseur, “CCPA cited in Hanna Andersson/Salesforce Breach Lawsuit” *Compliance Week* (6 February 2020). The California Consumer Privacy Act of 2018 came into force on 1 January 2020: Megan Graham, “California’s New Privacy Law Puts Billions Worth of Personal Data under Protection” *CNBC* (3 January 2020).

no standing to bring actions under the PDPA. Some other alternatives are considered below.

A. Recourse through the Personal Data Protection Commission

26 First, as mentioned above, it is possible for a complaint to be made directly to the PDPC.

27 Under s 50 of the PDPA, the PDPC may, upon complaint or of its own motion, conduct an investigation to determine whether an organisation is not complying with the provisions of the PDPA. The term “organisation” is defined to include individuals (including, for instance, ex-employees of that company).⁴⁸ The PDPC may, if satisfied that an organisation is not complying with relevant provisions of the PDPA, issue to the organisation such directions as the PDPC thinks fit to ensure compliance with the PDPA.⁴⁹ These directions include the stopping of collection and usage of personal data,⁵⁰ and the destruction of personal data.⁵¹ In some cases, the PDPC may also impose a financial penalty not exceeding \$1m on the organisation.⁵² The PDPC has even imposed fines on individuals.⁵³

28 However, while the PDPC may impose such financial penalties, the PDPA presently does not allow for the PDPC to order the organisation to pay compensatory or other damages to the data subject, unlike the litigation process through the Singapore courts. Based on the enforcement decisions published by the PDPC, it also appears that where the PDPC had decided to commence investigations in response to a complaint of a breach of the PDPA, the PDPC’s focus lay mainly in determining whether there was indeed a breach of the PDPA and issuing directions to the offending organisation for the regulatory purpose of securing compliance with the PDPA, as opposed to providing relief to the complainant. As such,

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

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

50 Personal Data Protection Act 2012 (Act 26 of 2012) s 29(2)(a).

51 Personal Data Protection Act 2012 (Act 26 of 2012) s 29(2)(b).

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

53 See, for example, *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319, *Re Ang Rui Song* [2018] PDP Digest 236 and *Re Chua Yong Boon Justin* [2017] PDP Digest 91.

a company wishing to seek relief for loss or damage suffered directly as a result of a breach of the data protection provisions of the PDPA may find that the right under s 32 of the PDPA (if available to companies) would have been a more suitable avenue as compared to lodging a complaint with the PDPC.

29 Additionally, in the case of organisations refusing to comply with any directions from the PDPC, there are several procedural steps that have to be taken before the PDPC can specifically compel the organisation to comply with the directions. For example, the PDPC would have to apply for its directions to be registered in the District Court,⁵⁴ by way of an *ex parte* originating summons⁵⁵ supported by affidavit.⁵⁶ Even after the PDPC has registered its directions with the District Court, the organisation can still apply to set aside such registration.⁵⁷ In such a scenario, execution of the directions will not be issued until the setting-aside application has been disposed of.⁵⁸

B. Civil proceedings under alternative causes of action

30 Second, companies that are not able to find a suitable means of seeking their desired type of relief under the PDPA itself may also consider civil proceedings via alternative causes of action. Data and information (which may include personal data) are also protected in Singapore by general common law obligations of confidentiality – therefore, a company may consider seeking relief on such grounds where a third-party recipient is subject to and has breached its duty of confidence towards such a company.⁵⁹ In certain circumstances, companies may also have the option of commencing civil proceedings due to a breach of contract, such as where

54 Personal Data Protection Act 2012 (Act 26 of 2012) s 30.

55 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 105 r 3.

56 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 105 r 4.

57 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 105 r 9.

58 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 105 r 10(2).

59 Briefly, apart from contractual confidentiality obligations, there are three elements that are normally required for a breach of confidence: (a) the information must be of a confidential nature; (b) the information must have been communicated in circumstances importing an obligation of confidence; and (c) there must be an unauthorised use of the information.

the party misusing the data in question has done so in breach of non-compete obligations imposed on it under such contract (such as under certain employment contracts). Depending on the factual circumstances and also the nature of the loss or damage in question, there may potentially also be sector-specific laws which companies may consider relying on.

31 In situations involving an ex-employee of a company, it may be possible for the company to make a claim against the ex-employee for breach of confidentiality, and seek remedies such as damages or injunction.⁶⁰ However, the availability of this cause of action ultimately depends on the facts, including the nature of the personal data in question, the exact wording of confidentiality clauses in the employment agreement or elsewhere, and the reasons for seeking protection,⁶¹ and it is therefore not a complete replacement for s 32 of the PDPA.

C. Other general considerations when determining whether to resort to litigation

32 Practically, companies should also note the potential implications of commencing civil proceedings in general. In particular, litigation is likely to be costly, time-consuming and damaging to the relationship between the parties due to the adversarial nature of proceedings. The reputation of the suing party may also be adversely affected. For example, in view of the increasing frequency of outsourcing of data management and processing activities by organisations and the implications of s 4(3) of the PDPA,⁶² it is highly possible for a company to find itself in a situation where it has suffered significant loss due to the acts or omissions of its third-party data intermediary and may wish to bring a civil action under the contract with

60 For example, *Jardine Lloyd Thompson Pte Ltd v Howden Insurance Brokers (S) Pte Ltd* [2015] 5 SLR 258.

61 For example, confidential information may have a limited shelf life. See *Tullet Prebon plc v BGC Brokers LP* [2010] EWHC 484 (QB) and *TFS Derivatives Ltd v Morgan* [2004] EWHC 3181 (QB).

62 Section 4(3) of the Personal Data Protection Act 2012 (Act 26 of 2012) provides that an organisation shall have the same obligation under the 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.

its data intermediary⁶³ – however, doing so would likely also expose the plaintiff company to negative publicity regarding the breach in question, such as for its failure to ensure that the personal data of its clients is safely protected, even if the act or omission resulting in the breach in question was not, practically speaking, within its control. The decision whether to seek redress via court proceedings should therefore be a carefully considered one based on a well-deliberated cost-benefit analysis.

33 Accordingly, whether to commence litigation, and the mode of litigation, depends very much on the facts. Generally, companies may wish to consider the following:

- (a) the nature of the breach of the PDPA;
- (b) who committed the breach of the PDPA;
- (c) who would be the party commencing the litigation (whether it is the corporate body or the data subject, and if it is the corporate body, whether the data subject is willing to be party to the litigation); and
- (d) what remedies are being sought.

34 These considerations would be instructive towards the mode of litigation and the cause of action relied upon, and whether or not litigation is even feasible.

63 The methods of dispute resolution which are relevant include any dispute resolution mechanism set out in the written agreement with the data intermediary, such as mediation, arbitration, litigation, *etc.*

Grounds of Decision

Re Tutor City

[2020] PDP Digest 170

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1806-B2228

Decision Citation: [2020] PDP Digest 170; [2019] SGPDPDC 5

Protection Obligation – Unauthorised disclosure of personal data – Insufficient security arrangements

Protection Obligation – Unauthorised disclosure of personal data – Lack of access controls

23 April 2019

BACKGROUND

1 As more organisations conduct business over the Internet, the volume and sensitivity of personal data collected online likewise increases. This case shows that when collecting documents containing personal data via a website, organisations should have in place reasonable security arrangements in the form of access controls to prevent unauthorised access to these documents to third parties. In particular, organisations should ensure that these documents are not unwittingly saved in folders that are accessible by the public.

2 On 8 June 2018, the Personal Data Protection Commission (the “Commission”) received a complaint from an individual (the “Complainant”) in relation to the publication of personal data belonging to 50 individuals on the organisation’s (the “Organisation”) website¹ (the “Website”). Specifically, images of the educational certificates of tutors using the Website were found to be publicly accessible by Internet users (the “Incident”).

1 <www.tutorcity.com.sg> (accessed 20 March 2020).

3 Following an investigation into the matter, I found the Organisation in breach of s 24 of the Personal Data Protection Act 2012² (“PDPA”). I set out below my findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

The Website

4 The Organisation is registered and managed by its sole proprietor (the “Sole Proprietor”). Through the Website, the Organisation provides matching services between freelance tutors and its prospective clients (eg, parents of students).

5 The Website lists freelance tutors and provides access to information about their educational qualifications, past experience and contact details. Freelance tutors agree to make such of their information publicly available and searchable on the Website when they sign on for the service. The Website also provides for an interested student or her parent to request for additional educational details from a tutor that they have identified. In order to provide this feature, tutors could upload their educational certificates onto the Website. The intention was for the tutors to approve each request to view their educational certificates, and by dint of this workflow, there was no intention to make the educational certificates publicly available or searchable outside the Website. The optional nature of this feature explains the low number of tutors who were affected, viz, 50 tutors out of a total of 13,283 tutors registered on the Website.

6 The Organisation had instructed a freelance web developer to design and develop the Website. Upon its completion in 2011, the Website was handed over to the Organisation and uploaded to a hosting server. It is admitted by the Sole Proprietor that:

- (a) the Organisation has been the sole party in charge of the Website after the handover;
- (b) the developer did not process any personal data on the Organisation’s behalf for the development of the Website; and

2 Act 26 of 2012.

- (c) the developer did not have any further involvement in the Website after it was handed over to the Organisation.

The Incident

7 As part of the Website's features, tutors interested in using the Organisation's matching service were given the option of voluntarily uploading up to three different educational certificates onto the Website. These certificates assisted the Organisation in matching the needs of the student in question to suitable tutors. These certificates were not intended to be made publicly accessible.

8 Notwithstanding this, all uploaded certificates were stored in the "/Public_html/directory" (the "Public Directory") of the Website's server within a sub-folder, "Public_html\tutor\tutor_image" (the "Image Directory"). Both directories were not secured with any form of access controls and were accessible by the public so long as the path to the relevant directory was known.

9 Investigations also revealed that the certificates were indexed by search engines like Google due to the lack of any measures taken to prevent automatic indexing of the Image Directory by web crawlers. This resulted in them showing up as search results on Google.

10 The Incident resulted in the disclosure of the following types of personal data of 50 individual tutors:

- (a) name of the individual;
- (b) NRIC number;
- (c) educational institution the individual attended; and
- (d) the grades the individual attained for each subject.

11 After being notified of the Incident, the Organisation took the following steps to prevent its reoccurrence:

- (a) it added a .htaccess file to the Image Directory that would restrict access to only the administrator; and
- (b) it deleted all the images stored in the Image Directory as of 8 June 2018.

FINDINGS AND BASIS FOR DETERMINATION

12 The issue for determination is whether the Organisation breached s 24 of the PDPA. Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the “Protection Obligation”).

13 As a preliminary point, I note that the Organisation, being the sole administrator of the Website, retained full possession of and control over the personal data that the Website collected at all material times. Although a developer was previously engaged for website development, the Sole Proprietor admitted that the developer did not process any personal data on behalf of the Organisation. Accordingly, the developer was not a data intermediary and the Organisation retained full responsibility for the IT security of the Website as well as the personal data contained therein.

14 Notwithstanding that the Organisation retained full responsibility over the Website’s security, other than instructing the developer to “make it safe”, the Organisation had paid little to no attention to the security of the Website. In this regard, the Sole Proprietor had provided the following statement:

From year 2011 to current, I did not implement any additional security measures to the website or its web directories as I am not tech-savvy and the current website had fulfilled my business needs. Therefore, even though the Personal Data Protection Act took effect in year 2014, I did not review my website to see if its security settings and measures are sufficient to protect the personal data of the tutors that had registered in my website. I did not think there was a need to review my website as I thought that Tutor City is a small business and no one would hack my website.

As for the security measures for the web directory, I do not have the knowledge of the exact settings or measures taken as I had pointed out earlier that I am not tech-savvy. When I commission the web developer to design the website, I gave him the business requirements and just told him to make it safe. I did not question on what sort of technical measures were to be used for the website. Before the website was uploaded to the hosting server, I did some testing on whether the features of the website were working correctly as intended but the testing was from a functionality angle and not to examine the security of the website. I wish to state that I am not aware of how the folders in the web directory are protected.

15 While the Website was developed and handed over to the Organisation before the PDPA came into force on 2 July 2014 (the “Appointed Day”), the Organisation continued to use the Website to collect personal data after the Appointed Day. As such, it was incumbent on the Organisation to take proactive steps to comply with its obligations under the PDPA. The following passage in *Re Social Metric Pte Ltd*³ is instructive:

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’.

16 In this regard, as can be seen from [14] above, no steps were taken after the Appointed Day by the Organisation or the Sole Proprietor to review the standard of security of the Website. The facts demonstrate that, prior to the Incident, the Organisation did not attempt to equip itself with knowledge of its data protection obligations under the PDPA. As mentioned above, the Organisation showed a lack of knowledge of the security arrangements over its Website. It did not:

- (a) communicate any specific security requirements to its developer to protect the personal data stored on the Website’s server, including instructing the developer to ensure that the uploaded certificates would not be accessible to the public;
- (b) make reasonable effort to find out and understand the security measures implemented by its developer for the Website;
- (c) attempt to verify that security measures to “make [the Website] safe” were indeed implemented by its developer; and
- (d) conduct any reasonable security testing (*eg*, penetration tests).

These demonstrate a fundamental lack of care by the Organisation over the personal data in its possession and/or under its control.

17 Related to the above, I note that the Sole Proprietor’s vague comment to its developer to make the Website safe does not constitute a security

3 [2018] PDP Digest 281 at [11].

measure. The Organisation could not have reasonably expected its developer to implement security measures that were adequate for the Organisation's purposes merely based on the Sole Proprietor's vague comment. The developer would not have known that the Organisation intended to protect the tutors' certificates from public access without the Organisation specifying this requirement.

18 While this palpable lack of detail may have been the norm before the Appointed Day, this is surely not the standard after the Appointed Day. The standard that is expected from organisations contracting professional services to build their corporate websites or other online portal is articulated in the Commission's *Guide on Building Websites for SMEs*.⁴ The Organisation ought to have reviewed the standard of security that had been implemented on the Website after the Appointed Day. In doing so, it should have delved into some degree of detail by providing its developer with the intended use cases and identifying risks and abuse that it could foresee. These do not require deep technical knowledge but do require the Organisation to have an understanding of how the Website will be used by itself and its customers. Had it reviewed the security standard implemented on the Website, it would have realised that all the certificates provided by the tutors were accessible publicly, when this was not the intention. The Sole Proprietor's claim that he lacked IT knowledge or tech-savviness is also not a defence against the Organisation's failure to take any steps to comply with the Protection Obligation.

19 As observed in the *Guide on Building Websites for SMEs*:⁵

5.5 Security Configuration Management

5.5.1 *Organisations should ensure, or require their vendor(s) to ensure, that the software and hardware components of the organisation's website are properly configured to prevent unauthorised access.* This includes reviewing operating systems, checking if appropriate antivirus/anti-malware software are in place and setting firewall rules to only allow authorised traffic. The configuration of each component should also be fully documented, kept up to date, and reviewed regularly.

5.5.2 *There should also be a plan for testing and applying patches and updates for the website's software and hardware components.* This includes having

4 Revised 10 July 2018.

5 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised 10 July 2018) at paras 5.5–5.6.

a process and person responsible to monitor new patches and updates that become available.

5.6 Security Testing

5.6.1 *Testing the website for security vulnerabilities is an important aspect of ensuring the security of the website. Penetration testing or vulnerability assessments should be conducted prior to making the website accessible to the public, as well as on a periodical basis (e.g. annually). Any discovered vulnerabilities should be reviewed and promptly fixed to prevent data breaches.*

5.6.2 Where organisations have outsourced the development of its website, they should require the IT vendor(s) to conduct the above security testing ... As a baseline, organisations may wish to consider using the Open Web Application Security Project (OWASP) Testing Guide and the OWASP Application Security Verification Standard (ASVS) to verify that security requirements for the website have been met.

[emphasis added]

20 The same guide goes on to add, amongst others, that:⁶

Access control is a critical part of the website's security arrangements. An effective access control scheme should be designed such that:

- Only authorised users (usually staff of the organisation) are allowed to access the website's administrative functions and personal data handled by the website ...
- All users should only be able to see the website functions and data that they are allowed to access ...

21 In the present case, I am advised that where documents containing personal data have to be stored in web servers, folder or directory permissions and access controls are a common and direct way of preventing their unauthorised access by public users and web crawlers. Depending on its circumstances, the Organisation could therefore have implemented any of the following reasonable technical security measures to prevent its Image Directory from being indexed by web crawlers:

- (a) First, the Organisation could have placed these documents in a folder of a non-public folder/directory. Access to such documents will then be controlled by the server's administrator. While this may not be ideal in complex servers with multiple

6 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised 10 July 2018) at para 6.2.1.

web applications – given that it may not be practicable for the server administrator to control access to all these files – this is not the case for the present Website.

- (b) Second, the Organisation could have placed these documents in a folder of a non-public folder or directory, with access to these documents being through web applications on the server. This could be done through PHP scripts. To access the data in the documents, users would have to first log into the web application.
- (c) Third, the Organisation could have placed these documents in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (*eg*, implement a password requirement or an IP address restriction). An index.html file could also be created within that sub-folder to show a HTML page with no content or a denial of access message. Any unauthorised user would then need the specific URL to access a document in the sub-folder. However, given that the Public Directory is the web root directory containing all the content to be displayed on the Website, it should not have overly restrictive access rights. This may pose some challenges for organisations seeking to balance access restrictions to specific documents against retaining accessibility to website content that is intended to be public.

22 It is up to each organisation to determine which security arrangements are the most suitable for its purposes, taking into account factors such as sensitivity of the personal data, size of the database and operational realities. The above are merely three potential technical security measures that organisations may implement to protect personal data.

23 On an even more basic level, the Organisation could, and should, have done proper housekeeping to ensure that all of its Website's publicly accessible folders did not contain files that were not meant to be publicly disclosed. Investigations disclosed that from the handover up till the occurrence of the Incident, the Organisation did not carry out any further updates or develop new security features for the Website. Although this did not contribute, in this case, to the Incident, it is nevertheless a separate breach of the Protection Obligation. I cannot emphasise enough the importance of putting in place maintenance processes to ensure regular

security patching as a security measure; regular archival of old data will also reduce the size of any breach that may arise and is therefore also an important aspect of the Protection Obligation. Data protection threats are constantly evolving, and patching is one of the common tasks that all IT system owners are required to perform in order to keep their security measures current against external threats.⁷

24 Besides the above, I note that the Organisation had taken the view that the security of the Website did not need to be reviewed because the Sole Proprietor did not think that it would be hacked. I would like to make it clear that the low likelihood of being hacked is not an acceptable reason for the failure to comply with the Protection Obligation. An organisation is required to put in place security arrangements to protect the personal data in its possession or control whether or not it believes that there is a likelihood of being hacked on the basis that it is a small organisation.

25 It is erroneous to think that the cybersecurity risk exposure of a business is commensurate with its business size. According to the “Singapore Cyber Landscape 2017” issued by the Cyber Security Agency of Singapore, almost 40% of the cyberattacks reported to SingCERT in 2017 targeted small and medium-sized enterprises (“SMEs”).⁸ A more recent study released in January 2019 by Chubb and YouGov has revealed that many SMEs in Singapore underestimate their exposure to cyber risks, and the existence of “a significant gap between the hard reality of cyber risk and how well small companies are prepared to deal with it”.⁹ Crucially, the same study observes that:

... it is becoming increasingly likely that if an SME has a security weakness, it will be targeted sooner rather than later. This is why, for cyber criminals, these

7 See also *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223 and *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160.

8 See Cyber Security Agency of Singapore, *Singapore Cyber Landscape 2017* <<https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecyberlandscape2017.pdf>> (accessed 20 March 2020).

9 Out of the 300 small and medium-sized enterprises in Singapore polled, 63% believed themselves to be less vulnerable than larger companies, yet 56% had experienced a cyber error or attack in the past 12 months: see Chubb, “Too Small to Fail? Singapore SME Cyber Preparedness Report” (2018) <https://www.chubb.com/sg-en/_assets/documents/chubb-sg-sme-cyber-preparedness-report.pdf> (accessed 20 March 2020).

businesses are the proverbial ‘low-hanging fruit’. Not only are they easy targets, they also offer a substantial cumulative payoff. In fact, *SMEs, with their low or no investment in cyber security measures, are actually the ideal, and subsequently the most common target for online crimes.* [emphasis added]

26 In the same vein, and as illustrated by the Incident as well as our previous decisions, data protection threats may not always come in the form of hacking incidents – the lack of access controls,¹⁰ which is something inherently within the Organisation’s powers to implement, system design errors¹¹ and human error¹² can similarly lead to a personal data breach incident. Organisations should therefore not take the security of their websites for granted simply because of the smaller scale of their businesses.

CONCLUSION

27 I find on the facts above that the Organisation did not make reasonable security arrangements to protect personal data in its possession or under its control against the risk of unauthorised access. The Organisation is therefore in breach of s 24 of the PDPA. I took into account the number of affected individuals, the type of personal data at risk of unauthorised access and the remedial action by the Organisation to prevent recurrence. I have decided to issue a warning to the Organisation for the breach of its obligation under s 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

10 See, for example, *Re Dimsum Property Pte Ltd* [2019] PDP Digest 282 and *Re Singapore Management University Alumni Association* [2019] PDP Digest 170.

11 See, for example, *Re COURTS (Singapore) Pte Ltd* [2019] PDP Digest 432; *Re Funding Societies Pte Ltd* [2019] PDP Digest 341 and *Re Jade E-Services Singapore Pte Ltd* [2019] PDP Digest 285.

12 See, for example, *Re Aviva Ltd* [2019] PDP Digest 145; *Re SLF Green Maid Agency* [2019] PDP Digest 327 and *Re National University of Singapore* [2018] PDP Digest 155.

Grounds of Decision

Re PAP Community Foundation

[2020] PDP Digest 180

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1807-B2434

Decision Citation: [2020] PDP Digest 180; [2019] SGPDPDC 6

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

23 April 2019

BACKGROUND

1 The organisation (“Organisation”) provides a range of services, including pre-school kindergarten services and senior care services. The central issue in this case, in so far as it is related to the Personal Data Protection Act 2012¹ (“PDPA”), is whether the Organisation had made reasonable security arrangements to protect the personal data of the students and students’ parents that it had in its possession and control at the material time.

MATERIAL FACTS

2 One of the many preschools under the Organisation’s management is the Sparkletots @ Kampong Chai Chee centre (the “preschool”). In the course of the year, the preschool would organise various school trips, sometimes with the participation of the parents. In preparation for these trips, the preschool would collect the parents’ personal data (including NRIC numbers) to allow for verification of the parents’ identity on the day of the trip.

1 Act 26 of 2012.

3 The present investigations arise from one such school trip. A few days before the trip was scheduled to take place, a teacher at the preschool sent a photograph of a consolidated attendance list to a “WhatsApp” chat group, reminding parents of the upcoming school trip. The attendance list contained personal data relating to the 15 students in that particular class and their parents, and included the contact numbers and NRIC numbers of five of the parents (the “Personal Data”). The “WhatsApp” chat group comprised the parents of students from that class.

4 The teacher who sent the photograph of the attendance list quickly deleted it after being alerted to the disclosure of personal data by one of the parents within the group chat. That same parent later lodged a complaint with the Personal Data Protection Commission (“PDPC”). PDPC thereafter commenced investigations into the incident.

THE DEPUTY COMMISSIONER’S FINDINGS AND BASIS FOR DETERMINATION

The relevant Personal Data Protection Act 2012 provisions

5 In respect of this matter, the relevant provision is s 24 of the PDPA. Section 24 requires an organisation to protect the personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the “Protection Obligation”).

Preliminary issues

6 It is not disputed that the Personal Data is “personal data” as defined in s 2(1) of the PDPA. There is no question or dispute that the Organisation falls within the PDPA’s definition of an “organisation”. There is also no dispute that the Personal Data was, at all material times, in the Organisation’s possession and under its control and that the Organisation was responsible for the Personal Data.

7 The key issue is therefore whether the Organisation had protected the Personal Data in its possession and under its control by making reasonable security arrangements to prevent unauthorised access and similar risks.

The Organisation failed to make reasonable security arrangements

8 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, I am of the view that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession and control, and has thereby breached the Protection Obligation under s 24 of the PDPA. This breach is attributable primarily to the Organisation's lack of specific policies or procedures in place to guide its employees on the use, handling and disclosure of personal data, especially in the context of communicating with parents.

9 It bears noting that "security arrangements", as envisaged in s 24 of the PDPA, encompass physical, technical and administrative measures to protect personal data. Such measures include data protection policies and procedures that employees must comply with in the course of their work. "Reasonable" in s 24 implies that the security arrangements in place are commensurate with the nature and volume of the personal data that the organisation possesses and/or controls.

10 In this regard, the Organisation has about 360 Sparkletots Centres with about 43,000 children enrolled. By the very nature of its kindergarten/preschool business, the Organisation collects, possesses and handles a significant amount of personal data of minors and parents alike. The everyday frequency of interaction between its staff and the parents of the children under the Organisation's care indicates also that specific policies or training would reasonably be expected to be put in place in order to guide staff on the PDPA obligations that will undoubtedly be engaged during their day-to-day activities. In the course of their work, the Organisation's staff are more likely than not to be placed in situations where the use and disclosure of personal data is crucial to the discharge of their duties, as it was with the case of obtaining consent for and organising the school trip in question.

11 The Organisation has admitted that it did not have such specific policies or procedures in place to guide its employees on the use and disclosure of personal data in their communications with the parents of students enrolled at the Organisation's preschools. While it had a data protection notice, this was a document that was intended to provide general information about how the Organisation handles personal data. It was meant for an external audience. It was not intended to provide detailed

guidance to its teaching and other staff on how they should handle personal data in the course of their work. Since the Organisation handles personal data of its students and their parents, the omission to provide detailed guidance to its teaching and other staff is an obvious gap in its security arrangements. To my mind, the Organisation needs to provide guidance to its employees in the area of communications and transmission of documents containing personal data, such as *via* messaging applications. The absence of such policies and procedures meant that the Organisation had little assurance that its employees were consistently performing their duties in a PDPA-compliant manner. This falls short of the standard of “reasonable security arrangements”.

12 That said, the Organisation had provided PDPA training to its employees at the preschool, including the teacher who had disclosed the attendance list. While PDPA training raises employees’ awareness of their obligations, this serves as a useful illustration that mere training alone cannot be a substitute for data protection policies and procedures in specific areas. Reasonable assurance against such incidents requires instituting and enforcing proper policies and procedures within an organisation, with training sessions acting as the medium to communicate such policies.

CONCLUSION

13 Based on the foregoing, I find that the Organisation has breached the Protection Obligation under s 24 of the PDPA.

14 Having found the Organisation to be in breach of s 24 of the PDPA, I am empowered under s 29 of the PDPA to give the Organisation such directions as I deem fit to ensure compliance with the PDPA.

15 In determining the appropriate directions to be imposed on the Organisation, I have taken into account the following mitigating factors:

- (a) the teacher in question acted swiftly in removing the Personal Data from the “WhatsApp” group; and
- (b) the number of individuals affected by the disclosure (15 students and 30 parents) was relatively small and the disclosure was constrained to the group of parents to whom the Personal Data pertained.

16 To its credit, the Organisation also acted swiftly to address its inadequate policies – a response which, in my assessment, carries mitigating value. The following remedial actions taken by the Organisation have therefore been taken into account:

- (a) immediate suspension of all “WhatsApp” chat groups following the disclosure;
- (b) expedited the implementation of a set of “Social Media Policy/Whatsapp chat group rules” that was already under development when the breach occurred;
- (c) rolled out a suite of other policies across the Organisation including a “Document Retention Policy” and an “Information Security Policy”; and
- (d) undertook the development of a practical employee handbook and conducted refresher training for its employees.

17 Having considered all the relevant factors of the case, I am of the view that these remedial actions have sufficiently addressed the current gap in policies and practices relating to the handling of personal data by the Organisation’s employees. I have therefore decided to issue a warning to the Organisation for breaching its obligations under s 24 of the PDPA, without further directions or imposing a financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Matthew Chiong Partnership

[2020] PDP Digest 185

Coram: Tan Kiat How, Commissioner

Case Number: DP-1709-B1138

Decision Citation: [2020] PDP Digest 185; [2019] SGPDPDC 7

Openness Obligation – Requirement to develop and implement policies and practices

Protection Obligation – Disclosure of personal data – Insufficient administrative security arrangements

3 June 2019

BACKGROUND

1 A member of the administrative staff of Matthew Chiong Partnership (the “Organisation”) mistakenly sent out e-mail correspondences meant for a client (the “Complainant”) to an incorrect e-mail address on two separate occasions. Additionally, a third e-mail correspondence was mistakenly sent by the managing partner and data protection officer of the Organisation (the “Managing Partner”) to the Complainant with an attachment which mistakenly contained the names of two other clients of the Organisation. The Commissioner found the Organisation to be in breach of its Protection Obligation and Openness Obligation under the Personal Data Protection Act 2012¹ (“PDPA”). The Commissioner’s findings and grounds of decisions are set out below.

MATERIAL FACTS

2 The Organisation is a Singapore-registered law firm which provides estate planning services and handles property transactions for its clients.

1 Act 26 of 2012.

3 On 28 August 2017, a member of the administrative staff of the Organisation sent an e-mail (“E-mail 1”) to two individuals informing them that the legal documents for their property refinancing had been prepared and were ready for signature. One of the e-mail addresses was incorrect as the administrative employee made an error in the e-mail address – as an example and only for illustration purposes, by typing <AAA@yahoo.com> instead of <ZAAA@yahoo.com>. The incorrect e-mail address was a valid e-mail address as the Complainant had sent a test e-mail to that e-mail address after E-mail 1 was sent and did not receive a mail delivery failed message. This mistake was identified by the sister of the Complainant (“Sister”), one of the intended recipients, who informed the Complainant. Once the Complainant informed the administrative employee, the administrative employee re-sent the e-mail to the Complainant. E-mail 1 disclosed information including the e-mail address of the Sister, the residential address of the Complainant and Sister, and the name of the bank in relation to the Complainant and Sister’s mortgage of their property.

4 The second incident occurred on 15 September 2017 when the same administrative employee sent an e-mail (“E-mail 2”), enclosing a letter addressed to a bank from the Organisation and a redemption statement issued by the bank, to the same incorrect e-mail address. E-mail 2 disclosed information including the full names, NRIC numbers, residential address, financial data such as the mortgage account information (consisting of the name of bank, account holders’ full names, loan account number, file reference number, name of security, and redemption statement of account for the month of September 2017) of the Complainant and her Sister. Following the two incidents, the Managing Partner apologised to the Complainant and Sister and offered: (a) a full refund of legal costs; and (b) to absorb all the disbursements incurred in handling the property transaction.

5 Subsequently, on 29 September 2017, the Managing Partner sent an e-mail (“E-mail 3”) to the Complainant and Sister enclosing two attachments: (a) a “Letter of Approval” from the Central Provident Fund (“CPF”) Board; and (b) a blank “Authorisation Use of CPF for Purchase of Private Property Form”. The Complainant noticed that there were two different documents contained within the Letter of Approval, and one of the pages reflected the full names of two other individuals (“Other Clients”), who were clients of the Organisation, and who were

unrelated to the Complainant's property transaction and unknown to the Complainant and Sister.

6 The table below sets out the three e-mails sent (collectively, the "E-mails") and the enclosed attachments (collectively, the "Attachments") along with a description of the corresponding information that was disclosed without authorisation.

	Type of Document	Information Disclosed
E-mail 1	Correspondence	<ul style="list-style-type: none"> • The Sister's e-mail address; • the Complainant's and Sister's residential address; and • the name of the bank in relation to the mortgage of the property.
E-mail 2	<ol style="list-style-type: none"> 1. A letter addressed to a bank from the Organisation 2. A redemption statement issued by the bank 	<ul style="list-style-type: none"> • The Complainant's and Sister's full names; • the Complainant's and Sister's NRIC numbers; • the Complainant's and Sister's residential address; and • financial data such as the mortgage account information which consists of the name of the bank, account holders' full names, loan account number, repayment information, and information relating to the collateral for the loan.
E-mail 3	<ol style="list-style-type: none"> 1. A "Letter of Approval" from the CPF Board 2. A blank "Authorisation Use of CPF for Purchase of Private Property Form" 	<ul style="list-style-type: none"> • The full names of Other Clients who were other clients of the Organisation, within two pages of documents which formed part of a larger ten-page legal document relating to the Other Clients.

THE COMMISSIONER'S FINDINGS AND ASSESSMENTS

Main issues for determination

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

- (a) whether the information disclosed by the E-mails and Attachments constituted personal data within the meaning of the PDPA;
- (b) whether the Organisation had implemented reasonable security arrangements to protect the personal data in its possession or under its control, as required pursuant to s 24 of the PDPA; and
- (c) whether the Organisation had put in place policies and practices relating to personal data, as required pursuant to s 12 of the PDPA.

Issue (a): Whether the information disclosed by the E-mails and Attachments constituted personal data

(i) The information disclosed in the E-mails and Attachments was personal data

8 Section 2(1) of the PDPA defines personal data as data, whether true or not, about an individual who can be identified from either that data, or from that data and other information to which the organisation has or is likely to have access. Given that the full names, residential address, NRIC numbers, e-mail addresses and financial data of the Complainant and Sister were disclosed, it would have been possible to identify the Complainant and Sister from the information contained in the E-mails and Attachments. Taking just the e-mail address of the Complainant as an example, given that it contained the partial name of the Complainant, it in itself would potentially allow a third party to identify the Complainant. The disclosure of the full names of the Other Clients in E-mail 3 would also have allowed a third party to identify these individuals. Accordingly, the information contained in each of the E-mails and Attachments or collectively, amounted to personal data within the meaning of s 2(1) of the PDPA.

(ii) The personal data contained in the E-mails and Attachments was sensitive in nature

9 The earlier decisions of the Commissioner have identified that certain information by reason of the context of its disclosure or by its very nature would be considered as personal data that is sensitive.² These include but are not limited to NRIC/passport numbers,³ financial data such as bank account details containing the name of the bank, the bank account number and the account holder's name,⁴ and insurance policy data such as the premium amount and type of coverage.⁵

10 As set out in the table at [6] above, the following personal data had been disclosed: the bank name, the NRIC numbers of the Complainant and Sister, loan account number of the bank, repayment information and collateral information. The disclosure of such information could have led to harm to the Complainant and Sister as such financial information could have exposed the Complainant and Sister to the risk of fraud and identity theft. As such, the personal data of the Complainant and Sister which had been disclosed, when taken as a whole, constituted sensitive personal data.

11 Since the Organisation is in the business of providing legal services and handles large volumes of personal data on a day-to-day basis, the Organisation and its staff should be vigilant in their handling of personal data. The fact that the same administrative employee managed to send the e-mails to the incorrect e-mail address on two separate occasions within a period under one month – *ie*, between 28 August and 15 September 2017 – despite being told of the mistake demonstrated that a culture of care and responsibility towards the handling of the personal data had not been sufficiently ingrained within the Organisation.

2 See *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [11].

3 *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 at [22]; and *Re Singapore Telecommunications Limited* [2018] PDP Digest 148 at [26].

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

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

Issue (b): Whether the Organisation has complied with its Protection Obligation under section 24 of the Personal Data Protection Act 2012

(i) Personal data of a sensitive nature is subjected to a higher standard of protection

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

13 In *Re Credit Counselling Singapore*⁶ (“*Re Credit Counselling Singapore*”) and *Re Aviva Ltd*⁷ (“*Re Aviva Ltd* [2017]”), the Commissioner opined that organisations are required to take extra precautions and ensure that higher standards of protection are accorded to sensitive personal data due to the actual or potential harm, and the severity of such harm arising from the unauthorised disclosure of such data.⁸ This point was again emphasised in the recent decision of *Re Aviva Ltd*⁹ where sensitive personal data was disclosed due to a lack of safeguards put in place to protect against the unauthorised disclosure of personal data in the organisation’s enveloping process. The Personal Data Protection Commission’s (“PDPC”) *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* urge organisations to “implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity”.¹⁰

14 Further, the Commissioner in *Re Credit Counselling Singapore* advised that suitable checks and controls be implemented before e-mails containing sensitive personal data are sent.¹¹ These may range from process-based supervision to technological controls like using the “mail-merge” function in Outlook. Credit Counselling Singapore had, after the data breach,

6 [2018] PDP Digest 295.

7 [2018] PDP Digest 245.

8 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [25] and [26]; *Re Aviva Ltd* [2018] PDP Digest 245 at [17] and [18].

9 [2019] PDP Digest 145.

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

11 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [29].

automated the process of sending e-mails using mail-merge software. The Organisation in this case should similarly consider putting in place a similar technological solution since it has to churn out standard form e-mails regularly.

15 However, the Commissioner “is not suggesting that organisations would need, for example, to have the added layer of supervision in all cases where emails containing personal data are being sent out ... organisations are to put in place security arrangements that are commensurate with the sensitivity of the data in question – a balance of considerations”.¹² The PDPC’s guide to preventing accidental disclosure when processing and sending personal data encourages organisations to have a process to double check and verify: (a) the recipients’ e-mail addresses; (b) whether the right attachments containing the correct personal data are attached; and (c) whether the attachments are for the intended recipients before sending the e-mails out.¹³ Therefore, implementing additional checks and controls when handling sensitive personal data is not a mandatory requirement but one that should be adopted where appropriate. Ultimately, the facts of the case and the type of personal data being handled will influence whether or not the current checks and controls implemented in the particular organisation are sufficient.

(ii) The Organisation failed to implement adequate security arrangements which led to the unauthorised disclosure of personal data

16 The Organisation explained that the unauthorised disclosure in the E-mails was caused by human error and failure to conduct thorough checks of the recipients’ e-mail addresses and the content of the attachments before sending out the E-mails to the recipients. For E-mail 1 and E-mail 2, the administrative employee had entered an incorrect e-mail address which the Organisation claims has never occurred when she had sent out electronic communications on previous occasions. For E-mail 3, the Letter of Approval was printed on recycled paper and scanned by an employee of the Organisation. However, the employee had scanned the Letter of Approval

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

13 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (20 January 2017) at para 2.1.

using the double-sided scanning mode which was the previous setting left on the scanner. As a result, a page containing the names of the Other Clients who were also clients of the Organisation was scanned together with the Letter of Approval.

17 The excuse that this was a one-off mistake by the employees and the Managing Partner of the Organisation, and not due to any lack of or failure to implement reasonable security arrangements pursuant to s 24 of the PDPA was duly considered by the Commissioner. This was an alternative position previously considered by the Commissioner in *Re Furnituremart.sg*.¹⁴ The Commissioner in *Re Furnituremart.sg* ultimately concluded that the organisation lacked the necessary policies and practices to protect personal data.¹⁵ Similarly, the Commissioner also takes the view in this case that the Organisation failed to implement reasonable security arrangements, and the incident could not be considered as a one-off inadvertent disclosure.

18 As a starting position, under s 53(1) of the PDPA, the Organisation is liable for the acts and conduct of its employees in relation to the unauthorised disclosure of the personal data. In response to the Commissioner's request of the details of the Organisation's security arrangements, the Organisation stated that: (a) all employees were briefed on the need to keep private and confidential personal data of their clients on a regular basis; and (b) all employees were advised to cut and paste e-mail addresses of clients from a legitimate source of information or click the "Reply" function to the e-mail sent from a client rather than type in the e-mail addresses. However, the Organisation was unable to provide any evidence of such briefings to its employees.

19 In *Re Aviva Ltd*, the Commissioner found 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".¹⁶ This case is no different. Therefore, the Commissioner finds that the Organisation's briefing to and/or giving advice to employees was by itself insufficient to prevent the unauthorised disclosure of personal data, particularly given the sensitive nature of the personal data.

14 *Re Furnituremart.sg* [2018] PDP Digest 175 at [11].

15 *Re Furnituremart.sg* [2018] PDP Digest 175 at [17].

16 *Re Aviva Ltd* [2018] PDP Digest 245 at [28].

20 Further, the nature of the Organisation’s services is a relevant factor to be taken into consideration. In *Re Credit Counselling Singapore*, the Commissioner observed that “it is foreseeable that there will be risks of inadvertent disclosure of sensitive personal data” where the organisation “routinely handles large volumes of sensitive financial personal data of individuals”.¹⁷ In the present case, the Organisation is a law firm and the staff handling conveyancing matters handle sensitive personal data on a day-to-day basis, and it was therefore foreseeable that there were risks of inadvertent disclosure of sensitive personal data. Given the nature of the Organisation’s work, the Organisation ought to be subject to a higher level of care and responsibility for its clients’ personal data.

21 The Commission released a *Guide to Data Protection Impact Assessments*¹⁸ which is intended to assist organisations interested in conducting data protection risk assessments. The Commissioner encourages the Organisation to carry out a data protection risk assessment on its conveyancing department, which should help identify and address the specific risks that exist in its operational processes. This will assist the Organisation to put in place effective risk mitigation measures.

22 Given the Commissioner’s findings above that the Organisation did not put in place adequate security arrangements to protect the personal data of its clients, it is hereby concluded that the Organisation was in breach of the Protection Obligation under s 24 of the PDPA.

Issue (c): Whether the Organisation has complied with its Openness Obligation under section 12 of the Personal Data Protection Act 2012

(i) The Organisation did not implement any policies or practices to protect personal data

23 The investigations revealed that the Organisation did not put any policies or practices in place to protect personal data. In *Re Furnituremart.sg*, the Commissioner decided that “the lack of a written policy is a big drawback to the protection of personal data ... Having a written policy is conducive to the conduct of internal training, which is

17 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [32].

18 Published 1 November 2017.

a necessary component of an internal data protection programme”.¹⁹ The Organisation’s claim that internal briefings were conducted to raise staff awareness was unsubstantiated by any supporting evidence. Nevertheless, even if verbal briefings were indeed given, this in itself would not be sufficient for the Organisation to discharge its obligations under s 12 of the PDPA. In general, an organisation should have some form of written policy or practice in place in relation to protecting personal data especially if the process is complex or if the organisation frequently deals with sensitive personal data on a daily basis. A well-drafted written policy has the advantage over verbal instruction of being a resource that can generally be subsequently relied upon to provide clarity on the appropriate procedures and controls to employees and help minimise the chance for any misunderstanding or miscommunication. This may take the form of written standard operating procedures in dealing with personal data which would set out the operational process of how employees should deal with personal data to prevent data protection breaches. For example, a process which implements the suggestion set out at [15] above may be set out in the form of a standard operating procedure.

24 Based on the above, given that the Organisation had not developed and implemented policies and practices that are necessary to protect personal data, it is the conclusion of the Commissioner that the Organisation is in breach of the Openness Obligation under s 12 of the PDPA.

REPRESENTATIONS

25 The Organisation, by way of e-mail dated 3 January 2019, requested that the imposition of the financial penalty amount be removed or that the amount be reduced. In this regard, the Organisation made the following representations:

- (a) the disclosure was not a deliberate act on the part of the Organisation or its staff;
- (b) the incidents related to one single conveyancing case involving two individuals;

19 *Re Furnituremart.sg* [2018] PDP Digest 175 at [14].

- (c) the Organisation waived all legal costs and expenses incurred in the matter in which it advised the Complainant;
- (d) the information disclosed is generally regarded as sensitive but that it had absolutely no interest to the recipient; and
- (e) the unauthorised disclosure was not due to lack of supervision and it was not possible to check all e-mail addresses every time there is an e-mail to be sent out. The employee who committed the error was 50 years old and probably has long-sightedness. She was not in the e-mail thread and so she could not have copied the e-mail address from the header of prior e-mails to the client. The said employee has since left the Organisation's employment.

26 The Commissioner in deciding to impose a financial penalty and on the appropriate quantum of the financial penalty had already taken into consideration the issues raised by the Organisation and as set out at [25(a)]–[25(c)] above.

27 With regard to the issue raised by the Organisation and set out at [25(d)] above, the Commissioner notes that the Organisation agrees that the information disclosed in these incidents is sensitive.

28 With regard to the issue raised by the Organisation and set out at [25(e)] above, the basis for the finding of a breach of the Organisation's obligation under s 24 of the PDPA was that the Organisation failed to implement reasonable security arrangements. In this regard, the Commissioner does not expect organisations to check the e-mail addresses every time there is an e-mail to be sent out. However, as explained above at [15], the Organisation ought to have implemented a considered process to verify that e-mails are correctly addressed to the intended recipient – the Organisation did not adduce any evidence of such a considered process. Nevertheless, the Commissioner has decided on compassionate grounds to reduce the quantum of the financial penalty set out in the preliminary decision issued to the Organisation, given that the member of staff who committed the error was advanced in age and long-sighted.

THE COMMISSIONER'S DIRECTIONS

29 The Commissioner is empowered under s 29 of the PDPA to issue directions as it thinks fit in the circumstances. This may include directing

the Organisation to pay a financial penalty of such amount not exceeding \$1m as the Commissioner thinks fit.

30 In assessing the breach and determining the directions to be imposed on the Organisation in this case, the Commissioner took into account the Organisation's dilatory conduct during investigations. It had been neither co-operative nor forthcoming in its responses to the Notice to Require Production of Documents and Information ("NTP") issued by the Commissioner as part of its investigations. The Organisation took a month to respond to the first NTP and second NTP despite being sent reminders by the Commissioner on several occasions:

- (a) The first NTP was sent on 12 December 2017 with a deadline to respond by 22 December 2017. The Organisation failed to meet the deadline and only on 2 January 2018, more than a week after the expiry of the deadline, did the Organisation write requesting for an extension of time to respond. The extension sought was up to 4 January 2018. The Organisation was granted an extension of time to respond by 10 January 2018. The organisation finally responded on 11 January 2018.
- (b) The second NTP was sent on 22 January 2018 requiring the Organisation to respond by 1 February 2018. The Organisation again failed to meet the deadline and did not even request for an extension of time to respond. The investigating officer had to call the Organisation on 6 February 2018 to ask the Organisation why it had failed to respond to the second NTP within the deadline. During this conversation, the Organisation requested for an extension of time of the deadline. The investigating officer informed the Organisation that she would issue a reminder with a deadline to respond by 15 February 2018. The reminder was issued on 7 February 2018. The Organisation failed to comply with this new deadline. In fact, no correspondence from the Organisation was received even by 20 February 2018. On 20 February, the investigating officer called the Organisation as a further reminder. Only after this did the Organisation respond to the second NTP on 23 February 2018.

31 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of

\$8,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court²⁰ in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

32 In addition, the Commissioner hereby issues the following directions to the Organisation:

- (a) to implement a data protection policy and internal guidelines or standard operating procedures to comply with the obligations under the PDPA;
- (b) for all employees of the Organisation handling personal data to attend a training course on the obligations under the PDPA and the Organisation's data protection policies; and
- (c) to complete the above directions within 60 days from the date of this decision and inform the office of the Commissioner of the completion thereof within one week of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

20 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re German European School Singapore

[2020] PDP Digest 198

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1712-B1471

Decision Citation: [2020] PDP Digest 198; [2019] SGPDPDC 8

Consent Obligation – Implied consent

Consent Obligation – Whether collection of personal data is beyond what is reasonable to provide product or service

3 June 2019

BACKGROUND

1 This case concerns a complaint made by the father (the “Complainant”) of a student¹ (“AB”) at the German European School Singapore (“GESS” or “Respondent”). The central issue raised in the complaint, in so far as it relates to the Personal Data Protection Act 2012² (“PDPA”), was that GESS had collected and used the personal data of AB without valid consent in the course of conducting a random drug test. GESS has not denied that it had collected the personal data of AB but has asserted that it did so with valid consent. The brief facts of the case are as follows.

2 On 6 December 2017, AB was selected by staff of GESS for random drug testing and asked to provide a hair sample by cutting for the drug test. This was done in accordance with GESS’s internal procedures and pursuant to its school bye-laws which provided that it may conduct drug testing at random or in cases of “proven suspicion”. When the Complainant found out about this later that day, he immediately contacted the principal of

1 As this individual is a minor, his name and the names of his parents are omitted from this decision.

2 Act 26 of 2012.

GESS (the “Principal”) via e-mail to object to the test being done on his son. The Complainant also requested that the results of the test be given to him in its unopened envelope, as received by the school.

3 In a turn of events, the drug test could not be conducted on AB’s hair sample as it apparently had not been stored correctly after it had been cut when it was sent to the overseas testing laboratory engaged by GESS to conduct the drug test.³ Following the e-mail correspondence between the Complainant and the Principal, the Complainant and his wife (“AC”) met with the Principal and other GESS staff on 12 December 2017 to discuss the matter. At the meeting, the Principal informed AB’s parents that AB was required to provide a second hair sample when he returned to school in January 2018.

4 The outcome of this discussion was that the Complainant and AC were informed by GESS during the meeting, and again by way of a letter dated 13 December 2017, that AB would be subject to immediate expulsion from the school if he did not provide a hair sample for the drug test on his first day back in school, or if the results of the test were positive.

5 The Complainant eventually sent another e-mail to the Principal on 7 January 2018 which stated that he permitted AB to give the second hair sample, albeit under his “profound protest”. In reply to this e-mail, the Principal reiterated GESS’s position that AB was required to give a hair sample for drug testing, failing which he would have to leave school. Thereafter, the Complainant sent a final e-mail emphasising that he had permitted AB to give the second hair sample.

6 On 8 January 2018, AB, accompanied by AC, presented himself at the Principal’s office at GESS. AC agreed to AB providing his hair sample for the purpose of drug testing and the school’s first aid officer proceeded to take a hair sample from AB.

7 On 11 January 2018, the Complainant submitted his complaint to the Personal Data Protection Commission (“PDPC”) that GESS had collected and used personal data of AB without consent. The Complainant

3 The drug test results on AB’s hair sample indicated “unable to complete” in respect of each of the drugs to be tested (listed in the results as cocaine, opiates, PCP, amphetamines and marijuana) and the reason stated was “INVALID SAMPLE – Flap A/B not sealed or improperly sealed”.

asserted that this was in contravention of ss 13 and 14 of the PDPA and that deemed consent (under s 15 of the PDPA) did not apply. The Complainant also asserted that GESS “expect[s] parents to consent to have their children randomly selected to take hair samples” and also that GESS “cannot argue that it is reasonable to do drugs testing in order to give a good education to its students”.

8 In its response to PDPC’s investigation into the matter, GESS sought to rely on agreements entered into between GESS and AC in 2006 and 2011. GESS also sought to rely on the Complainant’s correspondence with the Principal and AC’s verbal statements on 8 January 2018 to assert that the Complainant and AC had provided their consent for the collection of AB’s personal data. GESS also made various representations concerning the reasons for its drug testing policy.

THE DEPUTY COMMISSIONER’S FINDINGS

What is the personal data that is the subject of the complaint?

9 In his complaint, the Complainant raised the possibility of AB’s hair sample being part of his personal data, apparently on the basis that a hair sample contains DNA.⁴ In this case, GESS had not collected the hair sample for DNA testing and would not have obtained any information concerning AB’s DNA.

10 Nevertheless, the intention was to obtain through chemical analysis information about whether the individual had consumed controlled drugs by identifying traces found in the hair sample. It is this personal data that is the subject matter of the complaint. Further, it is clear that the hair sample was collected for drug testing and there would be a report produced by the testing laboratory which indicated the outcome of the test. The hair sample was sent to the testing laboratory on a “no-names” basis, that is, without identifying the individual to whom the sample belonged. As such, only GESS was able to match the drug test results with the student who had given the hair sample.

4 The Complainant stated in the third paragraph of the details of the complaint: “I realised that a hair sample contains DNA, and therefore qualifies as data in the list of examples you listed – which included DNA sample and Iris scans.”

What are the requirements for obtaining consent for the collection and use of personal data under the Personal Data Protection Act 2012?

11 Section 13 of the PDPA allows an organisation to collect, use or disclose personal data with the individual's consent unless an exception applied. Consent may be given by the individual or any person validly acting on behalf of the individual: s 14(4). However, s 14(2) read with s 14(3) invalidates any consent which requires an individual to give consent as a condition of providing a product or service, beyond what is reasonably necessary in order to provide the product or service. Section 15 of the PDPA contemplates the possibility that an individual may be deemed to have given consent through his voluntary act of providing personal data to the organisation for specific purposes; while s 16(1) of the PDPA provides that an individual may, at any time on giving reasonable notice to the organisation, withdraw any consent given, or deemed to have been given. Finally, organisations are held to a reasonable standard in meeting their responsibilities by virtue of s 11(1) of the PDPA.

12 As there are no written laws which require or authorise the collection of personal data without consent as in the circumstances of this case, GESS must therefore have either obtained consent under the PDPA for the collection and use of AB's personal data or AB must be deemed to have consented to such collection and use. For the purposes of this case, I would like to highlight the following principles which would apply under the PDPA:

- (a) The term "consent" under ss 13 and 14 – in contrast with "deemed consent" under s 15 – is not defined in the PDPA. In general, consent refers to any agreement to, or acceptance of, the matter which is being consented to.
- (b) The PDPA does not specify any particular manner in which consent is to be given under ss 13 and 14 of the PDPA. It is trite law that consent may either be express or implied:
 - (i) Express consent refers to consent which is expressly stated in written or verbal form.
 - (ii) Implied consent refers to consent which may be inferred or implied from the circumstances or the conduct of the

individual in question. Thus, *Black's Law Dictionary*⁵ defines “implied consent” as:

1. Consent inferred from one's conduct rather than from one's direct expression. – Also termed *implied permission*.
2. Consent imputed as a result of circumstances that arise, as when a surgeon removing a gall bladder discovers and removes colon cancer.

Likewise, in the High Court case of *Samsonite IP Holdings Sarl v An Sheng Trading Pte Ltd*⁶ which involved, amongst others, the question of whether certain backpacks were “put on the market with the [trade mark] proprietor's express or implied consent (conditional or otherwise)” within the meaning of s 29 of the Trade Marks Act,⁷ George Wei J observed that:⁸

The notion of ‘implied consent’ is a more difficult concept to grapple with [as compared to express consent], especially in terms of its application. In general, it can be characterised as consent which is not expressly granted by the proprietor, but rather inferred from his actions and/or the facts and circumstances of a particular situation.

In contrast to consent deemed by operation of law under s 15, this is a form of actual consent where the individual does, in fact, consent to the collection, use and disclosure of his personal data (as the case may be) although he has not expressly stated his consent in written or verbal form. It is a concept that is more expansive and malleable than deemed consent as its ambit is defined by the circumstances and conduct of the individual; but is necessarily more restricted in scope than express consent which is an expression of agreement of the range of purposes contemplated by the organisation to which the

5 10th Ed.

6 [2017] 4 SLR 99.

7 Cap 332, 2005 Rev Ed.

8 *Samsonite IP Holdings Sarl v An Sheng Trading Pte Ltd* [2017] 4 SLR 99 at [113].

individual agrees or accepts. (Parenthetically, the expansive scope of express consent is circumscribed by the requirement of reasonable appropriateness under s 18.)

- (c) For both of the above modes of giving consent to be effective under the PDPA, the requirements of s 14(1) of the PDPA must be met. For example, the individual must have been notified of the purposes for the collection, use or disclosure (as the case may be) of his personal data.⁹ In comparison, deemed consent under s 15 does not require that the individual must have been notified of such purposes: s 20(3)(a) of the PDPA. It suffices that the individual provided personal data for a purpose which may, or ought to, be known to the individual, or inferred from the surrounding circumstances.
- (d) Where an individual has given express or implied consent in the circumstances specified in s 14(2) of the PDPA (see above), such consent would be invalid. As stated in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*:¹⁰

12.15 Section 14(2) of the PDPA sets out additional obligations that organisations must comply with when obtaining consent. This subsection provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. The subsection also prohibits organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices.

9 An example of this is where an individual presents a credit card or charge card for the purpose of making payment for an online purchase. The individual expressly consents to the issuer bank collecting, using and/or disclosing his payment details to process his purchases. Deemed consent covers the disclosure of his payment details by the merchant to its acquiring bank. Implied consent enables the multiple layers of disclosure and use of his payment details by the financial institutions participating in the card scheme during the course of processing the payment. The concepts of deemed and implied consent operate in a mutually exclusive manner but may be daisy-chained.

10 Revised 27 July 2017, at paras 12.15–12.16.

12.16 Section 14(3) provides that any consent obtained in such circumstances is not valid. Hence an organisation may not rely on such consent, and if it collects, uses or discloses personal data in such circumstances, it would have failed to comply with the Consent Obligation.

- (e) Where an individual has given express or implied consent under the PDPA, deemed consent would not arise under s 15 of the PDPA. This is in view of the words in s 15(1)(a) which state that deemed consent may arise where the individual “without actually giving consent referred to in section 14, voluntarily provides the personal data to the organisation”.

Consent obtained by the German European School Singapore – Implied consent

13 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, I am of the view that GESS had obtained the necessary consent for the collection and use of AB’s personal data in connection with the drug test conducted on his hair sample.

Notification of purpose

14 As with other schools, GESS has in place various school rules and policies which it has established. Specifically, in relation to drug testing, para 5.8 of the Respondent’s school bye-law (“Bye-Law 5.8”) states as follows:

5.8 Drug Testing

The School shall conduct drug tests on students of Form 7 and above in cases of proven suspicion, as well as, at random. The Principal shall decide on the procedures of the test. If and when the first test shall be positive, and this is confirmed by a second test taken within a reasonable time-span, the respective student shall be expelled from the school immediately.

15 These bye-laws are made available to parents when they enrol their children in the school and are also available on GESS’s website through a parents’ portal set up by the school.

16 When considering Bye-Law 5.8, I note that it expressly states the outcome of a positive test, which is that the student in question will be expelled from the school. I am of the view that Bye-Law 5.8 sufficiently

specifies the purposes for which the drug test results would be used. Accordingly, I find that Bye-Law 5.8 has met the requirements of the PDPA in terms of notifying the individuals concerned of the purposes for the collection and use of their personal data.

17 During investigations, GESS sought to rely on the following documents to substantiate its assertion that it had obtained written consent for the collection and use of AB's personal data:

- (a) An agreement entered into by AC on 20 March 2006 to abide by the terms of GESS's bye-laws (including Bye-Law 5.8) (the "2006 Agreement").
- (b) An information letter provided to parents of GESS's students, including AC, on 31 October 2011 which included a reference and a link to GESS's bye-laws and which was accepted by AC on 1 November 2011 (the "2011 Information Letter").

18 The documents relied upon by GESS do not contain any express consent clause for the collection and use of personal data. This is unsurprising given that those documents predate the enactment of the PDPA. It is notable in this case that GESS had implemented a data protection policy following the enactment of the PDPA and it provided for express consent to be obtained for collection and use of various items of personal data for various purposes. However, GESS's data protection policy does not cover personal data collected for the purpose of drug testing and accordingly it has not sought to rely on its data protection policy in this case.

19 The 2006 Agreement comprises a set of documents entitled "Part 4 – Admission Forms" which were signed by the Complainant's wife on 20 March 2006.

20 Part 4.2 (entitled "Application Form") included the following paragraph which was signed and agreed to by the Complainant's wife:

I/We the undersigned request the enrolment of my/our child/ward/employee in accordance with the terms, conditions and the school rules of the German European School Singapore. I certify that all particulars furnished in this application are complete and accurate to the best of my/our knowledge, and that I/we will notify the School of any changes immediately. I/We acknowledge that the School is considering the application on the basis of the information I/we have provided.

21 Part 4.6 (entitled “Confirmation of Receipt of Documents”) included the following, which was also signed and agreed to by the Complainant’s wife:

By signing this confirmation, I/we hereby confirm that I/we have received the documents listed and that I/we agree to abide by their terms, and where appropriate make my/our child aware of their content.

<i>Title of Document</i>	
<i>School rules</i>	<i>Constitution of the School Association</i>
<i>School Fee Bye-Law</i>	<i>Terms and Conditions of Payments Fees</i>
<i>School Bye-Law</i>	<i>Bye-Law Governing the Education Principles</i>

[emphasis added in bold italics]

22 The 2011 Information Letter is a letter dated 31 October 2011 which had been sent by GESS to parents of its students. This letter informed parents of certain changes to their “Terms and Conditions”. These Terms and Conditions were found in a document entitled “Statutory Information” which included the school bye-laws. The following confirmation to the 2011 Letter was signed by AC on 1 December 2011:

I acknowledge receipt of the German European School Singapore Updated Terms and Conditions August 2011 and agree to accept the terms stated therein.

In my view, both the 2006 Agreement and the 2011 Information Letter each serve as sufficient notification under the PDPA, since, as noted above, Bye-Law 5.8 sufficiently identified the purposes for which students’ personal data (namely drug test results) were to be collected.

23 In the circumstances, I am of the view that AB’s parents had access to GESS’s school bye-laws and hence had been notified of the purposes for the collection and use of AB’s personal data in connection with the random drug testing administered by GESS.

Actual and/or implied consent (by conduct) to the collection of personal data in drug test results

24 GESS raised a number of specific instances where the Complainant and/or AC were alleged to have given their consent in written or verbal form, which I am satisfied to be the case on a review of the documents. Additionally, I am of the view that there is a more general principle that applies in this case. As the school’s bye-laws were made available to parents,

they must be taken to have agreed to enrol their children in the school on that basis. This is certainly the case in the present matter as AB has been enrolled in GESS for more than ten years.

25 I find that his parents' decision to enrol him, and to continue having him enrolled in the school for a substantial period, amounts to an acceptance of the school's bye-laws, including Bye-Law 5.8. This constitutes implied consent for the purposes of the PDPA and, as it was validly given by AB's parents, amounts to consent by AB pursuant to s 14(4) of the PDPA. A similar view was taken by the court in *GBN v GBO*¹¹ ("*GBN*") with respect to a school's confiscation of its student's mobile phone in accordance with its school rules. In that case, the school in question had confiscated the student's mobile phone as the student was found to have used the phone in contravention of the school's rule on mobile phones. The said rule further provided that the school will only return mobile phones which had been confiscated after a period of three months. The father of the student commenced court proceedings against the school alleging that the school's confiscation of the phone amounted to the tort of conversion. The court in *GBN*, in dismissing the father's proceedings, held:¹²

I also disagree with the plaintiff's assertion that he is not bound by the school rules. The plaintiff does not deny knowledge of the Phone Rule or the 3 January Letter. If the plaintiff took issue with the Phone Rule, the plaintiff could have enrolled his son in another school. Surely, as the defendant counsel submitted, by continuing to let his son study at the School, the plaintiff would have either expressly or impliedly agreed that his son would abide by the School's disciplinary policies and rules.

26 Similarly, by continuing to keep AB enrolled at GESS, the Complainant and AC have either expressly or impliedly agreed that AB would abide by the school bye-laws.

11 [2017] SGDC 143.

12 *GBN v GBO* [2017] SGDC 143 at [26].

Actual consent when AB provided his hair sample for the purposes of drug testing and collection of personal data

27 At this juncture, I should deal with the Complainant's e-mail of 7 January 2018 wherein he provided consent under protest for AB to undergo drug testing:

My principled objections to random drugs testing, as explained in my previous email ... remain unchanged, but my son's continued education at a school we otherwise like is more important, so [AB] will report to the front desk on Monday, under profound protest form [*sic*] my side:

It is my view that parents are ultimately responsible for their children's upbringing, and that we should be asked explicitly for consent to a policy that:

- invades our child's privacy
- has no relation to his performance, attitude, and behaviour at school
- has been ruled illegal in Europe.

Specifically, every parent should have the right to deny consent without any adverse impact on their child's school experience.

[emphasis added]

28 The Complainant's 7 January 2018 e-mail makes it clear that he agreed to allow AB to provide GESS with his hair sample for the purpose of the drug test in view of his continued desire for AB to remain and continue with his education at the school. Presumably, the purpose of giving consent under protest is to record the Complainant's objections to GESS's policy on random drugs testing on principle. His e-mail is premised on his "principled objections to random drugs testing" and that parents ought to be able to deny consent without any adverse impact on the child's school experience. The Complainant's protest does not and cannot be taken to mean that he is giving notice that he intends to challenge GESS's collection of personal data on the basis that his agreement under protest, without more, prevents such collection of personal data. This is made clearer on a review of the correspondence between GESS and the Complainant following the Complainant's said e-mail.

29 In response to the Complainant's e-mail of 7 January 2018, GESS replied on the same day as follows:

Dear [redacted],

Thank you for your mail. Our position has not changed. [AB] will not enter a classroom without giving a hair sample before doing so. If he is unwilling

to cooperate, he has to leave school at once. As you know. We [*sic*] are a private school and we have no obligations whatsoever to keep students who do not follow our policies.

30 The above e-mail is presumably an attempt by GESS to make clear that AB would have to provide his hair sample without any condition or AB's admission at the school would be terminated. This correspondence likely resulted from the uncertainty of the Complainant's intention agreeing to AB giving his hair sample under protest.

31 The Complainant then responded as follows:

Dear [redacted],

In your letter (attached), you asked [AB] to report to the front desk, and in my email this morning, I write to you that [AB] will do exactly that (albeit under my official protest, as stated).

So I am not sure why I receive this reply from you.

32 This makes it clear that the Complainant agreed to AB providing GESS with the hair sample, although the Complainant was clearly displeased about having to do so. Accordingly, AB presented himself later that day and underwent the collection of the hair sample for drug testing. In this regard, I note that GESS had asserted that AC also gave verbal consent when she accompanied AB to school on 8 January 2018.

33 The Complainant seeks to keep AB in GESS while cherry-picking from its bye-laws those that he does not wish to abide with. Bye-laws play an important role in shaping conduct within an organisation. In an educational institution like a school, it is untenable that parents are able to cherry-pick from its bye-laws in order to create a customised set of rules for their child. The organisation has the prerogative to justify that its bye-laws are reasonably necessary for maintaining conduct and discipline in the school, and to provide a safe educational environment. If the Complainant disagrees, it was always open to the Complainant or AC to have enrolled AB in another school which did not test its student for drugs. Accordingly, I find that GESS had obtained AB's consent for the collection and use of his personal data as required under s 13 of the PDPA. In coming to this conclusion, I bear firmly in mind the fact that AB's parents had not formally objected to the collection and use of AB's personal data until after he had been selected for random drug testing, even though he had been receiving his education in GESS for over a decade and AC had,

as a member of the GESS staff, known of the annual random drug tests that GESS conducts pursuant to its bye-laws.

Reasonableness – German European School Singapore’s collection of personal data found in AB’s drug test results is not beyond what is reasonable for the German European School Singapore to provide education services to AB

34 The Complainant also raised the issue that even if consent had been obtained by GESS, such consent would be invalid on the basis of s 14(2)(a) read with s 14(3) of the PDPA.

35 Broadly speaking, GESS is providing education services to AB and it is clear that GESS did not permit AB to be exempt from the random drug testing when he was selected. To the contrary, GESS clearly informed AB’s parents that he would be expelled from the school if he did not provide a hair sample and submit to the drug testing. Also, as set out above at [13]–[23], the Complainant had access to the school bye-laws and had been notified about the school’s random drug testing policy since at least by 20 March 2006 when AC entered into the 2006 Agreement with the school. In the context of the PDPA, this also amounts to a requirement that AB consent to the collection and use of his personal data (namely the drug test results, as stated earlier) by GESS for the purposes provided in Bye-Law 5.8. The question therefore arises as to whether GESS’s requirement for consent is beyond what is reasonable for the provision of education services by GESS to AB.

36 On this issue, I note that GESS asserted that the drug testing policy is instituted for a purpose which was reasonable and appropriate in the circumstances. In this regard, GESS stated the following in its response to PDPC:

With regard to query 5(g)^[13] of the Notice, the basis of GESS’ belief is as follows:

- i. GESS is registered as a society with its objectives and powers set out in its constitution;

13 Query 5(g) refers to the Personal Data Protection Commission’s query on the basis of the German European School Singapore’s assertion that its drug testing policy was instituted for a purpose which was reasonable and appropriate in the circumstances.

- ii. GESS has an open, long-standing, and firm policy on maintaining itself as a drugs-free institution;
- iii. In furtherance of this objective, GESS exercised its powers under its constitution to institute policies and bye-laws, including its drug policy;
- iv. As a school, GESS places paramount importance on the safety and welfare of its students, including maintaining itself as a drugs-free institution;
- v. GESS' drug policy is made known to and consented to by its students and/or their parents; and
- vi. GESS has in place clear guidelines and confidential procedures in implementing drug testing ...

37 GESS also asserted that the German Embassy of Singapore supported drug testing in schools and, in this regard, provided PDPC with a copy of a letter from the German Embassy of Singapore to the Respondent dated 1 March 2004 (in German together with GESS' translation). GESS' translation of the German Embassy's letter states that:

The foreign federal office makes the following statement regarding the intention to conduct drug testing at the German School Singapore and regarding the changes of the school bye-laws:

The Consideration of the German School Singapore, similar to other German schools abroad especially in the Asiatic region to introduce drug testing, has been welcomed. The German schools abroad develop their school regulations on the basis of the 'Guideline of the Standing Conference of the Ministers of Education and Cultural Affairs' (KMK) dated 15.01.1982. *Under this directive, schools are taking action to promote and ensure health care, including drug prevention. A coordination with the funding German authorities is not intended. With the enrolment of their child, the parents/guardians acknowledge the school regulations, and therefore also the provisions on health care and any regulations on drug prevention.*

The prerequisite for the introduction of a drug test policy is ... these procedures shall be embedded into an overall pedagogical concept to drug prevention. If such a concept is not included elsewhere in the school regulations, schools are requested to do so without further delay. For this purpose, the exchange of experience with other schools of the region in particular the German School Beijing is recommended, as they have included a drug policy as annex to their school regulations to, inter alia, *'save their students from addiction, keep the school free from addictive substances and to support students who are at risk of being addicted and their guardians to get away of the addiction,*

if necessary'. The German School Tokyo have similar plans. The background to such an overall pedagogical approach to drug prevention is the understanding of drug prevention as an educational task and not only as measurement to identify drug users.

[emphasis added]

38 As a general principle, schools have various responsibilities in relation to their students and these may extend beyond a purely pedagogical role. For example, they would also be responsible for ensuring the health and safety of students in the school environment. Hence, I am of the view that schools are best placed to determine the appropriate school rules and by-laws to establish in order to discharge their various responsibilities and create an environment that is conducive to meet the educational needs of their students. This may include implementing a policy which requires drug tests for certain students or in certain circumstances to ensure a safe environment and to detect behaviour and habits that may affect a student's scholastic performance. I am fortified by the views of the court in *GBN* where the court found that a school had the authority to implement and enforce school rules to maintain the discipline of its students as set out above at [25]. Just as in *GBN*, it was open to the Complainant in this matter to take AB out of GESS and enrol AB in another school.

39 It should also be highlighted that it was open to the Complainant to withdraw his consent on giving reasonable notice to GESS by virtue of s 16 of the PDPA. Had the Complainant withdrawn this consent, GESS would have had to inform the Complainant of the likely consequences of withdrawing the consent: s 16(2). Section 16(3) of the PDPA safeguards the Complainant by ensuring that GESS cannot prohibit his withdrawal of consent; but the Complainant will have to live with any legal consequences arising from such withdrawal, which in this case means that he has to take AB out of GESS and enrol him in another school. The application of these principles had been illustrated in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*.¹⁴

An individual wishes to obtain certain services from a telecom service provider, Operator X and is required by the telecom service provider to agree to its terms and conditions for provision of the services. Operator X can

14 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 27 July 2017) at para 12.45.

stipulate as a condition of providing the services that the individual agrees to the collection, use and disclosure of specified types of personal data by the organisation for the purpose of supplying the subscribed services. Such types of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data. The individual provides consent for those specified types of personal data but subsequently withdraws that consent.

The withdrawal of consent results in Operator X being unable to provide services to the individual. This would in turn entail an early termination of the service contract. Operator X should inform the individual of the consequences of the early termination, e.g. that the individual would incur early termination charges.

40 Clearly, the above finding is limited to the facts in this case and should not be taken as a general ruling that an organisation can in all cases justify a claim that it cannot provide services to an individual if the individual does not consent to the collection, use or disclosure of personal data. Any such finding is fact and context specific and must meet the same reasonableness test as set out at s 14(2)(a) and which is discussed above at [35]–[38].

Reasonableness – A reasonable person would consider it appropriate in the circumstances for the German European School Singapore to obtain a hair sample from AB by cutting his hair

41 Apart from whether consent to random drug testing in order to receive education from a school is reasonable, there is the related question whether the collection of personal data through the provision of hair sample by cutting is a reasonably appropriate means of implementing the random drug test policy. Section 11(1) of the PDPA imposes a general standard of reasonableness on organisations in meeting their responsibilities under the PDPA:

In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

42 To my mind, obtaining a hair sample by cutting in order to perform drug testing does not appear to me to be particularly invasive or unreasonable. Hair tests are contemplated in our anti-drug abuse laws as means of detecting suspected drug consumption: see s 31A of the Misuse of

Drugs Act.¹⁵ Also, obtaining a hair sample by cutting a few strands of hair is not invasive and does not ordinarily cause pain. I acknowledge that the random drug testing policy by GESS and the mandatory regime under the Misuse of Drugs Act are very different, and take care to emphasise that I refer to the Misuse of Drugs Act only to highlight that taking a hair sample to test for drug consumption is an acceptable method.

43 Accordingly, I find that the collection and use of AB's personal data in the circumstances of this case is not beyond what is reasonable for GESS to provide education services to AB and the collection of personal data through hair samples is a reasonably appropriate means to do so. As GESS has not contravened s 14(2) of the PDPA, s 14(3) does not apply and the consent obtained by GESS remains valid.

THE DEPUTY COMMISSIONER'S DECISION

44 In the circumstances, I find that GESS is not in breach of ss 13 and 14 of the PDPA as it had obtained consent for the collection and use of AB's personal data and this consent was valid and subsisting at the relevant time.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

15 Cap 185, 2008 Rev Ed.

Grounds of Decision

Re H3 Leasing

[2020] PDP Digest 215

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1803-B1859

Decision Citation: [2020] PDP Digest 215; [2019] SGPDPDC 9

Consent Obligation – Disclosure of personal data on social media without consent

6 June 2019

BACKGROUND

1 The complaint concerns the disclosure of personal data without consent by H3 Leasing (the “Organisation”). The Organisation is in the business of rental of motor vehicles in Singapore.

2 The complainant (the “Complainant”) was a member of the public who had come across a post on social media by the Organisation disclosing scanned images of the NRIC of another individual (“Affected Individual”). The personal data disclosed by virtue of this comprised of the full name, residential address, date of birth, NRIC number, NRIC photo and the thumbprint image of the Affected Individual (the “Personal Data Set”). On 8 March 2018, the Complainant filed a complaint with the Personal Data Protection Commission (the “Commission”) in relation to the disclosure of the Personal Data Set by the Organisation.

3 The key issue raised by the Complainant is whether the Organisation had the consent required under s 13 of the Personal Data Protection Act 2012¹ (the “PDPA”) to disclose the Personal Data Set of the Affected Individual in the manner and for the purposes which it did.

1 Act 26 of 2012.

4 Following an investigation into the matter by the Personal Data Protection Commission, I found the Organisation in breach of s 13 of the PDPA.

MATERIAL FACTS

5 On 15 December 2017, the Affected Individual rented a motor vehicle from the Organisation. He voluntarily provided a copy of his NRIC and entered into an agreement with the Organisation for that purpose.

6 Subsequently, the Affected Individual went into rental arrears and ceased contact with the Organisation. The Organisation was unable to locate him or the motor vehicle and made a police report concerning the apparent disappearance of the Affected Individual and the motor vehicle. The Organisation subsequently disclosed images of the Affected Individual's NRIC, which contained the Personal Data Set, through a public Facebook post to warn others about the Affected Individual and to solicit information from the general public on the whereabouts of the motor vehicle.

FINDINGS AND BASIS FOR DETERMINATION

7 Section 13 of the PDPA provides that an Organisation shall not collect, use or disclose personal data about an individual unless:

- (a) the organisation obtains the consent of the individual for the collection, use or disclosure of his personal data (in accordance with s 14 of the PDPA);
- (b) the individual is deemed to consent to the collection, use or disclosure of his personal data (in accordance with s 15 of the PDPA); or
- (c) collection, use or disclosure of his personal data is permitted or required under the PDPA or any other written law.

8 In this case, the rental agreement entered into by the Organisation and the Affected Individual did not specify any purposes for which the Organisation could disclose his personal data. There was no other document setting out such purposes and the Organisation admitted that it had not obtained the consent of the individual to disclose his personal data.

As such, I find that the Organisation did not have consent for the disclosure of the Personal Data Set in the manner, and for the purposes, that it did.

9 It is also clear to me that none of the exceptions to consent in the Fourth Schedule to the PDPA permit such disclosure. The purposes of the Organisation in making the public Facebook post were to warn others about the Affected Individual and to solicit information from the public on the whereabouts of the missing vehicle. These matters do not fall within any of the exceptions in the Fourth Schedule.

10 One question which may arise is whether the Organisation could have relied on the exception to consent in para 1(i) of the Fourth Schedule. That exception permits an organisation to disclose an individual's personal data without consent where it is necessary to do so in order for the organisation to recover a debt owed by the individual to the organisation. In my view, disclosure of the Personal Data Set via a public Facebook post would be too broad a disclosure and would not be necessary for the purpose of recovering a debt. Furthermore, disclosure of the scanned image of an NRIC (with all the data therein) in such a manner would be neither necessary nor appropriate.

11 As regards deemed consent, although the rental agreement between the Organisation and the Affected Individual did not expressly specify the purposes for which the Organisation could collect, use or disclose the Affected Individual's personal data, the Affected Individual had provided his personal data to the Organisation for purposes relating to the rental of the motor vehicle and deemed consent under s 15 of the PDPA would apply in respect of such purposes. The scope of deemed consent permits the Organisation to use and disclose the Affected Individual's personal data to other allied service providers as necessary to provide the primary service of motor vehicle rental. However, in my view, these purposes would not extend to permitting the Organisation to disclose his full NRIC details on social media for the purpose of warning others about the Affected Individual or soliciting information from the public on the whereabouts of the missing vehicle. Accordingly, deemed consent under s 15 of the PDPA does not apply to the disclosure in this case.

12 In the light of the above, I find that the Organisation had disclosed the personal data of the Affected Individual without consent and is therefore in breach of s 13 of the PDPA.

Conclusion

13 In assessing the appropriate enforcement action in this case, I took into account the following:

- (a) the Organisation's prompt action to remove the Personal Data Set from the public Facebook page;
- (b) the number of individuals affected; and
- (c) the impact of the breach.

14 Taking into account the factors listed above, I have decided to issue a warning to the Organisation for the breach of its obligation under s 13 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Option Gift Pte Ltd

[2020] PDP Digest 219

Coram: Tan Kiat How, Commissioner

Case Number: DP-1806-B2242, DP-1806-B2243 and DP-1806-B2244

Decision Citation: [2020] PDP Digest 219; [2019] SGPDPDC 10

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

6 June 2019

BACKGROUND

1 On 12 June 2018, the Personal Data Protection Commission (the “Commission”) was notified by the organisation (“Organisation”) of the unintended disclosure of up to 426 individuals’ personal data due to a coding error in its system. The Commission subsequently received complaints from two of the affected individuals on 12 and 13 June 2018, respectively.

2 Following an investigation into the matter, the Commissioner found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ (“PDPA”) and sets out below his findings and grounds of decision based on the investigations carried out in this matter.

MATERIAL FACTS

The portal

3 The Organisation maintains Uniqrewards (the “Portal”), an online portal through which national servicemen (“NSmen” or “NSman”) may

1 Act 26 of 2012.

redeem credits and gifts given by the Ministry of Defence (“MINDEF”) and the Ministry of Home Affairs (“MHA”) in recognition of their good performance during in-camp training or courses, or to celebrate certain events, such as the birth of a child. An NSman may log into the Portal and submit his redemption request, following which he would instantly receive a confirmation e-mail that his order is being processed (“Confirmation E-mails”). Besides the NSman concerned, the customer service team of the Organisation would also receive a copy of the Confirmation E-mail by way of blind carbon copy.

4 These Confirmation E-mails are generally sent via a service account linked to the Portal. The service account is hosted by an external vendor which has a password expiry policy of 180 days. While the employee concerned had previously reset the service account password before its expiry, he had failed to do so punctually in the latest round due to an oversight and a lack of reminders or warnings on password expiry. This led to 427 NSmen not receiving any Confirmation E-mails for their redemption requests submitted between 22 May 2018 and 24 May 2018. This issue was detected by the Organisation on 23 May 2018.

The incident

5 To rectify the issue, the Organisation wrote a separate programme script to regenerate and send out the Confirmation E-mails which the Portal had previously failed to send out due to the service account’s password expiration. The programme script was intended to achieve the following objectives:

- (a) accurately reflect the redemption request submitted by the NSman concerned and some of his basic details (*ie*, his login identification, e-mail address, delivery address and mobile number) on each regenerated Confirmation E-mail; and
- (b) send the Confirmation E-mail only to its intended recipient.

6 The format of these Confirmation E-mails was identical. To achieve objective (a), the programme script was meant to generate each of the 427 Confirmation E-mails by extracting the relevant details of the intended recipient from the Organisation’s backend database and including these details as part of the content of the e-mail. To achieve objective (b), the programme script was meant to address the Confirmation E-mail only to

the intended recipient's e-mail address. This process performed by the programme script was iterative, and all 427 Confirmation E-mails were to be generated in the same manner.

7 The programme script, however, did not behave as envisioned. While the content of each of these Confirmation E-mails was correctly generated by the programme script, the programme script left the e-mail address(es) of the recipient(s) of the preceding Confirmation E-mails in the "To:" field of the e-mail each time a new Confirmation E-mail was generated (the "Error"). It merely added on the intended recipient's e-mail address, instead of replacing the previous recipient's e-mail address with the intended recipient's.

8 In practice, this resulted in the first recipient of the Confirmation E-mail receiving the Confirmation E-mail that was intended for him as well as the Confirmation E-mails of all the other 426 recipients. The second recipient received the Confirmation E-mail which was intended for him as well as the Confirmation E-mails of the subsequent 425 recipients; the second recipient would not have received the Confirmation E-mail of the first recipient as the second recipient's e-mail address would not have been included in the Confirmation E-mail generated for the first recipient. Likewise, the third recipient received the Confirmation E-mail generated for him as well as the Confirmation E-mails generated for the subsequent 424 recipients; the third recipient would not have received the Confirmation E-mails generated for the first and second recipients as the third recipient's e-mail address would not have been included in the Confirmation E-mails generated for the first and second recipients. This pattern of addressing the Confirmation E-mails continued until the last recipient, who received only the Confirmation E-mail intended for him.

9 This Error resulted in the personal data of up to 426 NSmen being accidentally disclosed (the "Incident"). The personal data comprised the relevant NSman's:

- (a) login identification for the Portal;
- (b) e-mail address;
- (c) delivery address; and
- (d) mobile number.

10 After discovering the Incident, the Organisation took the following steps to mitigate the damage caused:

- (a) On 12 June 2018, the Organisation:
 - (i) e-mailed all the affected NSmen an apology and requested for them to delete all e-mails not intended for them from <redemption@uniqrewards.com>; and
 - (ii) notified the Commission of the Incident.
- (b) On 13 June 2018, all the affected NSmen received a text message from MINDEF and MHA, respectively, apologising for the Incident and requesting the deletion of the same e-mails.
- (c) In July 2018, the Organisation gave all the affected NSmen a gift voucher worth \$80 as a gesture of apology.

11 In addition to the above, the Organisation introduced the following further steps to prevent the recurrence of the Incident:

- (a) All future changes to the Portal would be subjected to a secondary check during the development testing stage. Specifically, the person conducting integration testing would be required to print out the expected output in the development environment and have it validated by a checker before starting the user acceptance test.
- (b) All coding scenarios would have a separate person reviewing the source code written by the developer.
- (c) The Organisation began work to enhance the Portal's backend system to allow Confirmation E-mails to be resent directly.
- (d) The Organisation introduced a standard operating procedure to document the process of resending Confirmation E-mails. Under this procedure, only authorised users, with the approval of the Organisation's data protection officer, may resend Confirmation E-mails. An audit trail would also be created during this process.
- (e) The Organisation would deploy an application, Sonarcloud, to analyse the quality of source codes. Sonarcloud would be used to detect bugs, vulnerabilities and code smells during the development process.

FINDINGS AND BASIS FOR DETERMINATION

12 As a preliminary point, s 4(1)(c) of the PDPA excludes an organisation which acts on behalf of a public agency in relation to the collection, use or disclosure of personal data from Pts III to VI of the PDPA

(*ie*, the data protection provisions). Nevertheless, the Commission's investigations revealed that the Organisation was a subcontractor of MINDEF and MHA and was not engaged by both public agencies to act on their behalf as a data intermediary. As such, s 4(1)(c) does not apply to the Organisation and the Organisation is required to comply with the data protection provisions of the PDPA.

13 The main issue for determination is whether the Organisation breached s 24 of the PDPA. 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.

14 As the administrator of the Portal, the Organisation had full possession and control over the personal data that the Portal collects, uses, discloses and processes at all material times. Accordingly, the Organisation had full responsibility for the security of the Portal, any changes to it, as well as the personal data processed by it. In this regard, the Commissioner found that the Organisation had failed to conduct sufficient testing before rolling out the programme script.

15 In this case, software testing (*ie*, development testing and user acceptance testing) was carried out on the programme script prior to its actual implementation. Investigations revealed a fundamental flaw in designing the test scenarios. The test scenario consisted of generating all 427 test e-mails but instead of picking up the recipient e-mails from a list of e-mail addresses, each e-mail was hardcoded to be sent to the same internal e-mail address. Unsurprisingly, the Error, which would only have manifested itself if there was more than one recipient, was not detected. A more thoroughly designed test scenario that more closely approximated the anticipated real-world deployment environment could have included:

- (a) the use of several test e-mail addresses;
- (b) the programme script retrieving these test e-mail addresses from a database (*eg*, the main database of e-mail addresses or a database of e-mail addresses created for the job) instead of using a single hardcoded e-mail address; and
- (c) the programme script being used to send the Confirmation E-mails to the retrieved test e-mail addresses.

16 For the reasons above, the Commissioner finds the Organisation in breach of s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

17 Given 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 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.

18 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account the following mitigating factors:

- (a) the Organisation voluntarily notified the Commission of the breach;
- (b) the Organisation fully co-operated with the Commission's investigations;
- (c) the Organisation took prompt action to mitigate the effects of the breach by informing the affected individuals via e-mail on the same day (12 June 2018) and offering them a voucher worth \$80 in July 2018; and
- (d) the Organisation took prompt corrective action to resolve the vulnerability and further remedial measures to enhance its backend system to prevent the recurrence of similar incidents.

19 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to pay a financial penalty of \$4,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court² in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

2 Cap 322, R 5, 2014 Rev Ed.

20 The Commissioner has not set out any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Ncode Consultant Pte Ltd

[2020] PDP Digest 226

Coram: Tan Kiat How, Commissioner

Case Number: DP-1712-B1471

Decision Citation: [2020] PDP Digest 226; [2019] SGPDPDC 11

Protection Obligation – Unauthorised access and modification to personal data – Insufficient security arrangements

6 June 2019

BACKGROUND

1 This is a case of six students using teachers' login credentials to access Victoria School's NTRIX school management system ("NTRIX"). The students were able to obtain the login credentials of teachers by exploiting an SQL vulnerability found in NTRIX (the "Incident"). Ncode Consultant Pte Ltd ("Ncode" or the "Organisation") supplied NTRIX to various schools, including Victoria School. Victoria School is a school organised and conducted directly by the Ministry of Education ("MOE").

2 On 5 December 2017, the Government Technology Agency of Singapore on behalf of MOE reported to the Personal Data Protection Commission (the "Commission") that the NTRIX system for Victoria School suffered a total of 84 unauthorised logins (the "Unauthorised Logins") between 3 August to 17 October 2017.

3 Following an investigation into the matter, the Commissioner found Ncode in breach of s 24 of the Personal Data Protection Act 2012¹ ("PDPA").

1 Act 26 of 2012.

MATERIAL FACTS

4 Ncode is a school administrative system developer and has been working with schools since 1994. NTRIX is a web application/portal managed by Ncode. There were three levels of users (a) students/parents; (b) teaching/non-teaching employees; and (c) administrator. By logging in with their respective passwords, teachers could enter examination scores and comments. Students and parents could also log in to view results.

5 At the time of the Incident and Unauthorised Logins, there were 2,792 records of students' personal data stored as part of Victoria School's instance of NTRIX. In each record, the students' personal data may include all or some of the following information: student name, admission number, residential address, mobile number, parents' names and contact details, subject proficiency rating at primary six, current examination scores at Victoria School and examination summary ratings (collectively, "Personal Data").

6 The Incident and the Unauthorised Logins exposed the Personal Data to risk of unauthorised access, use and modification. In addition, the unauthorised users could view confidential data of the students (*eg*, examination results before they are published). There were also 11 instances of modification of examination results for ten students. The investigations revealed no evidence of mass data exfiltration. The unauthorised modifications to the examination results were rectified by Victoria School, and there was no impact on the students' grades.

7 Ncode took the following remedial actions after discovery of the unauthorised access on 11 October 2017:

- (a) 12 to 13 October 2017: two-factor authorisation ("2FA") was introduced for Victoria School's employee logins to NTRIX.
- (b) 14 to 17 October 2017: Ncode identified and fixed the SQL injection² vulnerability that led to the Unauthorised Logins.

2 SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (*eg*, to dump the database contents to the attacker).

- (c) 21 October 2017: Ncode fixed all high-risk items found using OWASP ZAP³ active scan.
- (d) February 2018: Ncode informed all of its developers of the proper use of the security scanning tools VCG⁴ and OWASP ZAP. Ncode also installed automatic security scans and committed to conducting penetration testing as scheduled. In addition, Ncode’s data protection officer was instructed to review Ncode’s data protection policies.
- (e) March 2018: Ncode initiated the use of the correct features of automatic testing tools to actively test NTRIX for vulnerabilities.

THE COMMISSIONER’S FINDINGS AND BASIS FOR DETERMINATION

8 It is not disputed that the Personal Data is “personal data” as defined in s 2(1) of the PDPA. There is no question or dispute that Ncode falls within the PDPA’s definition of “organisation”. In the course of investigations, it was determined that Ncode was at all material times an independent third-party service provider to, and therefore was not acting on behalf of, MOE. Neither did Ncode raise the applicability of s 4(1)(c) at any time. In the circumstances, s 4(1)(c)⁵ of the PDPA does not apply.

Whether Ncode Consultant Pte Ltd complied with its obligations under section 24 of the Personal Data Protection Act 2012

9 Ncode was appointed to supply NTRIX to Victoria School as well as to set up, host and maintain NTRIX for Victoria School for the period 1 January 2017 to 31 December 2017 pursuant to an invitation to quote (“ITQ”) and the annexed “Quotation Conditions of Contract” read

3 OWASP ZAP (short for Zed Attack Proxy) is an open-source web application security scanner.

4 VCG (short for Visual Code Grepper) is an automated security review tool that handles C/C++, C#, Java, VB and PL/SQL.

5 Section 4(1)(c) of the Personal Data Protection Act 2012 (Act 26 of 2012) provides that “any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data” is not subject to the obligations under Pts III–VI of the Act.

together with Ncode's ITQ submission dated 14 December 2016 (collectively referred to as the "Contract"). Pursuant to the Contract, Ncode assisted Victoria School to upload the relevant databases containing the Personal Data for use with NTRIX and was obliged to comply with the MOE IT Security Specifications for School-managed Systems ("MOE IT Security Specs").

10 It is not disputed that Ncode's scope of work in the Contract included processing the Personal Data in NTRIX nor that it was in possession or control of the Personal Data. The Commissioner therefore finds that Ncode was acting as a data intermediary of Victoria School.

11 In the circumstances, Ncode had an obligation to put in place reasonable security arrangements to protect the Personal Data which was in its possession and/or under its control.⁶

12 Based on the investigations, there were two causes of the Incident and the Unauthorised Logins:

- (a) The exploitation, by one of the students, of the NTRIX' SQL injection vulnerability using a publicly available SQLMap tool to discover usernames and encoded passwords stored as part of NTRIX for employee and administrator logins. The passwords were then decoded and shared with other unauthorised users. This allowed the unauthorised users to gain access to the Personal Data and make changes.
- (b) The passwords found in the NTRIX system were not encrypted or hashed but were merely encoded in Base64. The passwords were easily decoded with a publicly available online decoder. Once this was done, they were linked to the usernames of the account holders. The decoded passwords could then be used to access the web application with a legitimate existing user account.

13 SQL injection vulnerability was, at the material time, and still is, a common and well-known information technology security threat used by hackers to access computer systems without authorisation. The SQLMap injection program used in the Incident did not require sophisticated

6 See s 4(2) read together with s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012).

knowledge in order to exploit the SQL injection vulnerability found in NTRIX. Detecting and fixing such a basic form of SQL injection vulnerability did not require specialist IT security skills but is within the expertise of the average software developer.

14 Further, para 16.4(g) of the MOE IT Security Specs specifically highlighted SQL injection vulnerability flaws and required such flaws to be rectified in the application system by Ncode before deployment. Regular security vulnerability scanning was also required under para 21.13 of the MOE IT Security Specs. Security scanners would have detected the SQL injection vulnerability found in NTRIX if used with the correct settings and features. However, Ncode failed to use the features available in security scanning tools like VCG and OWASP ZAP to actively detect common software vulnerabilities like the SQL injection vulnerability in this case.

15 Also, encoding passwords using Base64 is not a reasonable security arrangement to protect the Personal Data, as these may be easily reversed with a publicly available online decoder as was done in this case. In the case of *Re ComGateway (S) Pte Ltd*,⁷ the Commissioner found that encoding a shipment ID using Base64 is not an actual means of encryption. Base64 is a common and simple encoding scheme, easily decoded through publicly available decoding tools. ComGateway was found in breach of s 24 of the PDPA because the URL of the shipping webpage unique to each customer (by virtue of the shipment ID encoded in Base64) could be easily manipulated and ComGateway did not put in place security measures to address this vulnerability.

16 Investigations showed that the two causes of the Incident as well as the Unauthorised Logins were due to the inexperience of Ncode's engineers in IT security. An engineer with reasonable IT security knowledge would have (a) detected and fixed the basic form SQL injection vulnerability; and (b) applied adequate password protection measures for all passwords.

17 In responses to notices to produce, Ncode admitted that its engineers were unfamiliar with IT security and lacked basic understanding of the correct settings/features of security scanners needed to detect SQL injection vulnerability. These engineers also did not understand the basic features of encoding, hashing and encrypting to protect passwords properly. In fact,

7 [2018] PDP Digest 308.

para 8.4 of the MOE IT Security Specs required Ncode to ensure its technical and security personnel are trained in IT security and are aware of the security implications of the work performed. There is no excuse for Ncode's failure to train the relevant employees in IT security.

18 The investigations also revealed that the NTRIX system had other vulnerabilities which were undetected. These included broken session management⁸ and cross-site scripting.⁹ While these vulnerabilities were not exploited in the Incident or in respect of the Unauthorised Logins, they exposed the Personal Data stored in NTRIX to unauthorised access.

19 In addition, the Incident not only resulted in unauthorised access, but also unauthorised modification of students' examination results. While there was no harm suffered by the students as Victoria School managed to rectify the unauthorised modifications, this will not always be the case. The Commissioner would like to emphasise that the failure to put in place reasonable security arrangements to prevent unauthorised modification is a serious breach of an organisation's obligation to protect personal data. Changes to examination results could have had an impact on the academic performance of the students affected.¹⁰ In this regard, an attacker may stealthily make unauthorised modifications which may be difficult to detect, and consequentially cause significant harm. Possible security arrangements to prevent unauthorised modification include automatic notification when changes are made to static historical personal data or the need for a higher level of access rights to make any changes to such personal data, given the significance of examination results to students' academic performance.

20 For the reasons above, the Commissioner finds Ncode in breach of s 24 of the PDPA.

8 A weakness that allows a hacker to either capture or bypass authentication methods due to improper management of sessions.

9 Enables a hacker to inject client side scripts allowing the hacker to bypass access controls.

10 See Elena Chong, "ASEAN Scholar at SMU Jailed 16 Weeks for Hacking into Professor's Computer and Changing Grades" *The Straits Times* (8 November 2017), where changes were made by the accused person to give himself better grades.

THE COMMISSIONER'S DIRECTIONS

21 Given the Commissioner's findings that Ncode is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue Ncode such directions as it deems fit to ensure compliance with the PDPA. This may include directing Ncode to pay a financial penalty of such amount not exceeding \$1m.

22 In assessing the breach and determining the directions, if any, to be imposed on Ncode in this case, the Commissioner took into account the following aggravating factors:

- (a) Ncode's business includes processing of minors' personal data. It is therefore imperative that reasonable security arrangements ought to have been in place to protect the personal data of minors.
- (b) Ncode should have easily detected and rectified the well-known SQL injection vulnerability that existed in its basic form.

23 The Commissioner also took into account the following mitigating factors:

- (a) Ncode co-operated fully with the investigations; and
- (b) there was no evidence of mass exfiltration of personal data as a result of the Incident or the Unauthorised Logins.

24 Having considered all the relevant factors of this case, the Commissioner hereby directs Ncode to pay a financial penalty of \$30,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court¹¹ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

REPRESENTATIONS MADE BY THE ORGANISATION

25 The Organisation in its letter to the Commission dated 19 December 2018 stated that while it concurred with the facts and findings set out in this decision, it had requested for a reduction of the financial penalty

11 Cap 322, R 5, 2014 Rev Ed.

quantum. It made this request on the basis that it had co-operated fully with investigations as well as taking prompt action to remediate the breach.

26 The Commissioner had already taken into consideration the above points in coming to its decision on the financial penalty.

27 The Organisation had also referred to the financial penalties imposed on other organisations. However, the facts in the decisions referred to by the Organisation were not identical to the facts in this case.

28 In particular, the Organisation cited three cases in which the organisations that were in breach of their obligations under the PDPA were imposed a financial penalty that was less than that imposed on the Organisation. The cases cited by the Organisation were *Re ComGateway (S) Pte Ltd*,¹² *Re WTS Automotive Services Pte Ltd*¹³ and *Re Propnex Realty Pte Ltd*.¹⁴ However, the major difference between these three cited cases and the current matter is that this matter, unlike the cases cited by the Organisation, included the personal data of minors. Organisations ought to protect the personal data of minors to a higher standard and the unauthorised access or disclosure of personal data of minors is an aggravating factor when the quantum of financial penalty to be imposed is determined.

29 The Commissioner is, therefore, of the view that the financial penalty imposed in this case is justified, in particular given the aggravating factors set out above at [22].

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

12 [2018] PDP Digest 308.

13 [2019] PDP Digest 317.

14 [2017] PDP Digest 171.

Grounds of Decision

Re Starhub Mobile Pte Ltd and others

[2020] PDP Digest 234

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1609-B0229

Decision Citation: [2020] PDP Digest 234; [2019] SGPDPDC 12

Consent Obligation – Withdrawal of consent

6 June 2019

BACKGROUND

1 The present matter arose from a complaint made by an individual mobile subscriber (“Complainant”), in relation to the current industry practice of mobile network operators charging for the provision of caller number non-display (“CNND”) services. The CNND service is offered on a per-line basis affecting all outgoing calls made using a particular telephone number. When activated by a subscriber, the CNND service essentially prevents the subscriber’s telephone number from being displayed on call recipients’ devices.

2 The organisations are the three mobile network operators in Singapore (“Organisations”). They offer a range of telecommunication services to subscribers, in particular, mobile telephony services. They also offer CNND as an optional value-added service to their subscribers. All the Organisations share a common practice of charging subscribers for the provision of CNND services, although the precise charges differ from Organisation to Organisation.

3 The key question which has to be determined in this case is whether s 16 of the Personal Data Protection Act 2012¹ (“PDPA”) prohibits organisations from imposing charges for the provision of CNND services.

1 Act 26 of 2012.

The findings and grounds of decision based on the Commission's investigation are set out below.

MATERIAL FACTS

4 The Complainant is an individual subscriber of StarHub Mobile Pte Ltd ("StarHub")'s mobile services. He had written to StarHub to request the withdrawal of his consent to the disclosure of his telephone number to parties receiving his calls.

5 In response, the Complainant was informed by StarHub that if he wished to prevent his telephone number from being displayed to call recipients, he would need to activate StarHub's CNND value-added service. He was also informed that a one-time activation charge and monthly recurring charges were applicable.

6 The Complainant was not agreeable to pay the charges for activating the CNND value-added service. He expressed the view that, as he was exercising his right under the PDPA to withdraw consent to the disclosure of his personal data, he should not be required to pay any charges for the CNND value-added service in order to prevent his telephone number from being displayed to call recipients.

7 Against this backdrop, the Complainant raised this matter to the Commission. As the practice of charging for CNND services is common to all the Organisations, the Commission commenced an investigation into the practices pertaining to the CNND services of all three Organisations.

Conveyance/withholding of calling party's telephone number from recipient

8 In the course of its investigation, the Commission obtained a range of information from the Organisations pertaining to the manner in which a calling party's telephone number is conveyed to a call recipient during a telephone call, as well as details pertaining to the implementation of the CNND value-added service. Investigations disclosed the following:

- (a) All mobile and fixed line operators in Singapore are interconnected using international telephony signalling protocols, *eg*, signalling system No 7 and session initiation protocol. Under the arrangements for interconnection adopted

by the Organisations, a caller's telephone number will be passed on by the caller's network operator to the receiving network operator as part of the conveyance of a telephone call.

- (b) The transmission of the calling party's telephone number by the calling party's operator to the recipient's operator takes place regardless of whether the calling party has activated CNND services. The calling party's network does not remove the calling party's telephone number from being transmitted. The difference in handling the caller's number lies in indicators as to whether the phone number should be displayed or hidden from the recipient.
- (c) If the call recipient has activated caller ID (also known as caller line identity or "CLI") services, the recipient operator's network will forward the calling party's telephone number to the recipient's device. Otherwise, the calling party's telephone number will not be forwarded to the recipient's device, and the recipient's device would not display the incoming caller's telephone number. Currently, the vast majority of Singapore mobile subscribers have enabled CLI services.
- (d) The flow of the caller's telephone number from the caller to the caller ID display at the call recipient's device when the call recipient has activated the CLI services for his telephone line takes place in the following manner:
 - (i) When the caller dials the call recipient's telephone number using his phone, the call will be routed from the caller's originating local exchange to the recipient's local exchange, which could be in the same or different telecommunication company's network, based on the pre-planned call routing arrangement. The originating local exchange will be able to determine which telephone communications company the call recipient has subscribed to and will try to establish a call with the designated recipient's local exchange through the adopted signalling protocols.
 - (ii) If the call recipient's telephone is connected to the call recipient's telephone network, after the call is routed successfully, an acknowledgment awaits the call recipient to pick up the call, which is typically translated to the

ringing of the telephone. At this stage, the caller's telephone number is reflected on the call recipient's telephone as caller ID display. The call is considered established after the call recipient picks up/accepts the call.

- (iii) Where the caller has activated CNND for his telephone line or where the call recipient has not activated CLI for his telephone line, the caller's ID will not be shared with the call recipient.
- (e) The CNND services offered by the Organisations allow callers' telephone numbers to be hidden from call recipients even if these call recipients have subscribed to caller ID services. The Organisations' CNND services are based on recommendations promulgated by the Telecommunication Standardisation Sector of the International Telecommunication Union ("ITU-T"). In addition to per-line CNND, it is also possible to offer CNND on a per-call basis although the Organisations have not made CNND available on a per-call basis. Each of the Organisations imposes its own set of charges on its subscribers for the CNND service. Typically, the charges consist of a combination of a one-time activation charge and monthly recurring charges.
- (f) If a calling party has subscribed for CNND services, when a telephone call is initiated, the calling party's network operator would transmit a CNND indicator, together with the calling party's telephone number, through the originating telephone network to the recipient's network operator. The function of the CNND indicator is to mark the caller's telephone number as "Presentation Restricted", which would notify the recipient's network operator not to forward the calling party's telephone number to the recipient's device.
- (g) In order for the calling party's telephone number to be withheld from the recipient, the recipient network operator's co-operation is needed to honour the CNND indicator, by recognising the indicator and withholding the calling party's telephone number from the recipient's device.
- (h) As such, the successful withholding of the calling party's telephone number from the call recipient is ultimately dependent on co-operation between the caller's network operator and the recipient network operator. In this regard, the

Commission understands that the Organisations have adopted common standards for CNND services, and as between themselves will typically honour one another's CNND indicators.

FINDINGS AND BASIS FOR DETERMINATION

9 The key issue to be determined in this case is whether the Organisations have contravened s 16 of the PDPA by requiring individual subscribers to pay charges for the CNND value-added service, in order to withhold their telephone number from being disclosed to call recipients.

10 In addressing the aforementioned key issue, it is pertinent to briefly address a couple of preliminary issues that were raised in the course of the Commission's investigation into this matter, namely:

- (a) whether telephone numbers constitute personal data; and
- (b) whether express consent is required for the disclosure of telephone numbers to call recipients.

Whether telephone numbers constitute personal data

11 In some of their representations to the Commission, the Organisations suggested that mobile telephone numbers do not constitute personal data for the purposes of the PDPA. In this regard, the Organisations asserted that a call recipient would not be able to identify a calling party simply by looking at the telephone number displayed.

12 I do not think that that such an assertion accords with the definition of "personal data" under the PDPA. Section 2 of the PDPA defines "personal data" to mean:

... 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.*

[emphasis added]

13 In relation to whether telephone numbers constitute personal data, the Commission has stated in the *Advisory Guidelines for the Telecommunication Sector* that:²

Telephone numbers and International Mobile Equipment Identity ('IMEI') numbers

2.3 Where an individual is identifiable from the data, such as a combination of the individual's name, address and telephone number, then such data is personal data. In cases where the individual cannot be identified from that data alone (such as a device identifier in itself), such data may still be personal data if the organisation has or is likely to have access to other information that will allow the individual to be identified when taken together with that data ...

2.4 In the telecommunication context, *an individual's mobile telephone number is likely to be personal data as it may uniquely identify, or be uniquely associated with, that individual ...*

[emphasis added]

14 Additionally, the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* also identify personal mobile telephone numbers as a *unique identifier*, and hence personal data on its own:³

5.8 Certain types of data can on its own, identify an individual, for instance biometric identifiers which are inherently distinctive to an individual, such as the face geometry or fingerprint of an individual.

5.9 Similarly, data that has been assigned to an individual for the purposes of identifying the individual (e.g. NRIC or passport number of an individual) would be able to identify the individual from that data alone.

5.10 Such data which, on its own, constitutes personal data, is referred to as 'unique identifier' in these guidelines. Data that the Commission generally considers unique identifiers include:

- ...
- Personal mobile telephone number
- ...

15 Mobile use in Singapore has grown in leaps and bounds. Just in terms of figures alone, there were altogether 8,381,900 mobile subscriptions in

2 Personal Data Protection Commission, *Advisory Guidelines for the Telecommunication Sector* at paras 2.3–2.4.

3 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* at paras 5.8–5.10.

Singapore as of March 2018, and a mobile population penetration rate of 149.3%.⁴ It was also reported that seven in ten Singaporeans use social media on mobile, which, according to the survey, is double the global average.⁵ Given the multitudinous uses of the mobile today, mobile numbers have increasingly been used as a form of identification or verification of individuals, including for online transactions, mobile payments and social networking. This works on the general premise that an issued mobile number is unique, and no two same mobile numbers should be in operation at the same time. Hence, a mobile number acts as a unique address at which individuals may be contacted or receive messages or information on their mobile phones. In this regard, mobile numbers double up as a unique identifier of the individual.

16 This role of a personal mobile telephone number as a unique identifier is further strengthened by the mobile telephone number portability policy such that an individual is able to retain and keep his mobile telephone number when he switches to another service provider. This is one of the reasons that caller ID is popular with mobile phone subscribers – a subscriber is able to identify the caller through the caller’s telephone number if the subscriber had programmed the caller’s telephone number in his telephone directory.

17 Also, when one of the Organisations uses a subscriber’s personal mobile telephone number, for example, to establish a telephone call or for logging call data for billing purposes, that Organisation is using that personal mobile telephone number as a unique identifier of the individual subscriber.

18 There is, however, a distinction between land lines and mobile telephone numbers. The foregoing discussion is concerned with mobile

4 See Infocomm Media Development Authority, “Statistic on Telecom Service for 2018 Jan – Jun” (4 September 2019) <<https://www.imda.gov.sg/infocomm-media-landscape/research-and-statistics/telecommunications/statistics-on-telecom-services/statistic-on-telecom-service-for-2018-jan>> (accessed 30 April 2020).

5 See Angela Tan, “7 in 10 Singaporeans Use Social Media on Mobile, Double Global Average: Survey” *The Business Times* (24 January 2017) <<http://www.businesstimes.com.sg/consumer/7-in-10-singaporeans-use-social-media-on-mobile-double-global-average-survey>> (accessed 25 March 2020).

telephone numbers. A land line terminates at premises that are, more likely than not, shared: *eg*, residence of a family or place of business of an organisation. It is the recognition of this key distinction that the aforementioned advisory guidelines limit the policy guidance to treating mobile telephone numbers as personal data without adopting a similar approach for land lines. Consumers and organisations also do not treat land lines as personal.

19 From the perspective of the call-originating network, the Organisation transmitting its subscriber's mobile telephone number will be transmitting personal data since it has full subscriber details. From the perspective of the recipient of the call, the reality today is that a significant number of calls will be matched with an address book entry in the recipient's mobile phone and will thus identify the caller, or the recipient may recognise the number. Hence, I am satisfied that the guidance set out in the advisory guidelines referred to above would be applicable in the context of the present case, and that it would be entirely relevant and reasonable to proceed with the analysis in this case on the basis that subscribers' mobile telephone numbers constitute personal data.

Deemed consent for disclosure of subscriber identity to telephone call recipients

20 The *Advisory Guidelines for the Telecommunication Sector* set out the following guidance in relation to consent and the withdrawal of consent for the disclosure of a subscriber's telephone number to receiving parties:⁶

Provision of subscriber identity for calls or text messages

3.8 Currently, when a subscriber who is an individual makes a telephone call or sends a text message, his telephone number (which may be personal data relating to him) would typically be disclosed to the receiving party and both the subscriber and receiving party's telecommunication operators, unless the subscriber had chosen to have his telephone number 'blocked'/ 'unlisted'. Telecommunication operators may wish to obtain the consent of the individuals for the purpose of such disclosures to recipients of his calls and messages.

6 Personal Data Protection Commission, *Advisory Guidelines for the Telecommunication Sector* at paras 3.8–3.11.

3.9 *Even if the telecommunication operators do not obtain such actual consent, given established practice, the Commission is of the view that a subscriber who opts to have an ‘unblocked’/ a ‘listed’ telephone number would typically be aware that the telephone number would be collected, used or disclosed for the purpose of identifying that subscriber to other parties. Where the telephone number is personal data relating to a subscriber, a subscriber with an ‘unblocked’/ a ‘listed’ telephone number initiating a call or sending a message may be deemed to have consented to the collection, use or disclosure of the number for the purpose of identifying himself to the receiving party, since the subscriber would have voluntarily provided the data, and it would be reasonable for the subscriber to have done so.*

3.10 *Conversely, a subscriber who has opted for a ‘blocked’/ an ‘unlisted’ number at the outset would not be considered to have consented to the collection, use or disclosure of the number for that purpose. A subscriber with an ‘unblocked’/ a ‘listed’ telephone number who subsequently applies to ‘block’/ ‘unlist’ that telephone number would be considered to have withdrawn consent for the collection, use or disclosure of that telephone number for the purpose of identifying himself to other parties when making a call or sending a message.*

3.11 Where an individual subscriber is deemed to have given consent for disclosure of his telephone number by one telecommunication operator to another telecommunication operator for the purpose of identifying himself to the recipient of his call or message, consent may be deemed to have been given to the collection, use or disclosure of the telephone number by that other telecommunication operator for the same purpose. Alternatively, consent may not be required if the purpose for collection, use or disclosure of the personal data falls within an exception, such as when it is required or authorised under written law.

[emphasis added]

21 I understand that currently the Organisations obtain express consent from subscribers for the collection, use and disclosure of their telephone numbers for the purpose of identifying them to receiving parties. This is a good practice although, as the *Advisory Guidelines for the Telecommunication Sector* establish, not strictly necessary. A subscriber who has opted for an “unblocked” or “listed” telephone number may be deemed to have consented to the collection, use or disclosure of his telephone number for the purpose of identifying himself to recipients of his calls.⁷ It naturally

7 Section 15(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) and Personal Data Protection Commission, *Advisory Guidelines for the Telecommunication Sector* at para 3.9.

follows that the Organisations would be able to rely on deemed consent to collect, use or disclose the subscriber's telephone number for the purpose of identifying the subscriber to call recipients.

Whether the Organisations have contravened section 16 of the Personal Data Protection Act 2012

22 Turning to the key issue raised in this case, s 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to be given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose.

23 Section 16(3) of the PDPA is particularly relevant, and states that an organisation:

... shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section *shall not affect any legal consequences arising from such withdrawal*. [emphasis added]

24 Section 16(3) of the PDPA may be seen as comprising two limbs, namely that:

- (a) an organisation shall not prohibit individuals from withdrawing consent; and
- (b) any legal consequences arising from such withdrawal shall not be affected.

25 It is necessary to construe both limbs of s 16(3) of the PDPA holistically. While s 16(3) of the PDPA is clearly intended to ensure that individuals are not prohibited from exercising their right to withdraw consent, it also expressly preserves any legal consequences arising from such withdrawal.

26 It is also pertinent to refer to s 11(1) of the PDPA, which imposes a general standard of reasonableness on organisations in meeting their responsibilities under the PDPA. Section 11(1) of the PDPA states:

In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

27 At this juncture, it should be highlighted that the provision of CLI services serves important societal purposes, including helping to reduce calls made to harass or scam individuals and to speed up law enforcement

investigations where a caller's telephone number is required for the purposes of criminal investigations. Additionally, given that most mobile telephone subscribers have CLI and that over-the-top telephone services such as calls made through smartphone applications do not provide the ability to the caller to mask his telephone number, the provision of CLI services has become a baseline expectation of all users of modern mobile telephone networks: call recipients expect to know the identity of the caller. Consumers' expectations to be able to identify an incoming caller as a basic functionality is also clearly embedded into the design and manufacture of mobile phones as mobile phone manufacturers universally incorporate the ability to display caller ID as a basic and essential feature of modern mobile phones. This functionality is integrated with the contact list functionality such that display caller ID is matched with contact details whenever a call is received, and the caller's name is displayed by the mobile phone when the call is connected. This modern convenience enables the subscriber to decide whether to answer the call from an identified contact; and some subscribers prefer not to take calls when the display caller ID does not match a known contact.

28 Under the signalling standards adopted by fixed and mobile network operators in Singapore, a caller's telephone number will be transmitted by the calling party's network to the receiving party's network by default as part of the conveyance of a telephone call.

29 In order for calling parties to withhold their telephone numbers from being displayed to call recipients (the vast majority of whom currently have caller ID enabled), action has to be taken on the part of the Organisations, in terms of transmitting and giving effect to the relevant "Presentation Restricted" indicator.

30 Against this backdrop, I understand from the Organisations' representations that, for CNND services to be implemented and offered as an option to subscribers, the Organisations have had to invest in relatively complex IT systems which are, amongst other things, able to automatically and in real time instruct the mobile network to either implement or deactivate the CNND depending on whether the caller is a CNND subscriber and which would be able to manage the customer sign-up for CNND and the database of CNND customers. Regular and continuous tests and updates to the IT systems are also required to ensure that CNND continues to work accurately when there is an update to interconnected

systems, whenever new handsets are introduced into the Singapore market by the Organisations, when new roaming partners are on-boarded by the Organisations and when new technologies and platforms (such as VoLTE and VoWiFi) are deployed.

31 Perhaps in a nod to the infrastructure investment and operational costs required in order to provide consumer choice in both CLI and CNND services, the International Telecommunication Union (“ITU”) provides charging principles for supplementary services such as for the charging of both CLI and CNND services, but has left it to the individual member country to formulate its own policy decision with respect to charging for such services. The ITU is an agency of the United Nations specialising in information and communication technologies and, amongst other things, allocates global radio spectrum and satellite orbits. In its ITU-T Rec D.232, ITU provides for charging principles for supplementary services as follows:

2.1 Number Identification

This subclause provides charging principles for the supplementary services, Calling Line Identification Presentation (CLIP), Calling Line Identification Restriction (CLIR), Connected Line Identification Presentation (COLP), Connected Line Identification Restriction (COLR) and Malicious Call Identification (MCID). Detailed description of the services are provided in Recommendations 1.251.3 (CLIP), 1.251.4 (CLIR), 1.251.5 (COLP), 1.251.6 (COLR and 1.251.7 (MCID).

2.1.1 Charging principles

Innovation of the display or restriction service may be charged for by:

- a) Inclusion in the rental charges raised against customers; or
- b) The setting of a separate subscription charge;
- c) A per event charge; or
- d) Combinations of a) to c).

32 Given established practice as discussed above and the inherent nature of a telephone call, whereby a calling party’s telephone number is by default transmitted to the recipient network operator and typically forwarded to the call recipient’s device, it would not be unreasonable for the network operator to charge a reasonable fee for the costs it incurs to provide the CNND and restrict the number from being disclosed to the call recipient. Also, given the competitive marketplace in the provision of telecommunications services in Singapore, market forces can be expected to determine the range of service charges that any of the Organisations will be

able to impose for the CNND service. The relevant charges for the Organisations' CNND services are publicly accessible and can be obtained by subscribers relatively easily, and any charges payable by individual subscribers to the Organisations for CNND services would have a legal basis stemming from the contract between subscribers and the Organisations.

33 In summary, users of modern mobile telecommunications services expect to be able to identify a caller and mobile telephone handset manufacturers have incorporated CLI as a basic and essential feature. CLI now plays a societal role, enabling consumers to order their private lives and exercise choice in how they wish to be contacted or to decline taking calls. In order to provide consumers with this choice, significant ongoing investment has to be made by the Organisations to maintain CNND services for its subscribers. The ITU also recognises that there may be a need to charge for both CLI and CNND services. In our domestic market, the price of these services is contained by competitive market forces. With the provision of CNND services as a value-added service, consumers have access to a paid service to restrict the sharing of their personal mobile phone numbers.

34 Given the consumer expectations and reliance on CLI and how CLI is fundamentally embedded into the design and operation of mobile telephone systems and handsets, and the additional infrastructure investments and operational costs required to provide consumer choice for CLI and CNND, it is not unreasonable that the Organisations impose a reasonable charge for these services. I have no doubt that a reasonable person would consider it appropriate for the Organisations to charge a caller to prevent his telephone number from being displayed to the call recipient, failing which the Organisation may inform the subscriber that the Organisations are unable to provide the caller with telecommunications services if he wishes to withdraw such consent. An example which illustrates the application of this can be found in the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, which states:⁸

An individual wishes to obtain certain services from a telecom service provider, Operator X and is required by the telecom service provider to agree

8 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* at para 12.45.

to its terms and conditions for provision of the services. Operator X can stipulate as a condition of providing the services that the individual agrees to the collection, use and disclosure of specified types of personal data by the organisation for the purpose of supplying the subscribed services. Such types of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data. The individual provides consent for those specified types of personal data but subsequently withdraws that consent.

The withdrawal of consent results in Operator X being unable to provide services to the individual. This would in turn entail an early termination of the service contract. Operator X should inform the individual of the consequences of the early termination, e.g. that the individual would incur early termination charges.

35 I am therefore of the view that the provision of CNND is less a means to withdraw consent for the disclosure of the caller's personal mobile telephone number to the call recipient than a separate service to allow a caller to maintain anonymity. Accordingly, where an individual subscriber requests his telecommunications service provider to mask his telephone number when he calls another phone number, the Organisations are in compliance with s 16 if they inform the subscriber that he may do so by subscribing and paying for CNND services, failing which the Organisation is unable to provide the telecommunications service to the subscriber. By doing so, the Organisations would have informed the subscriber of the legal consequences arising from such withdrawal pursuant to s 16(2) of the PDPA.

36 Having carefully considered all the relevant circumstances of the present case, and for the reasons set out above, I find that the Organisations have not breached s 16 of the PDPA in respect of the charges imposed on subscribers for providing CNND value-added services, and that no further action is required in this matter.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Skinny's Lounge

[2020] PDP Digest 248

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1806-B2267

Decision Citation: [2020] PDP Digest 248; [2019] SGPDPDC 13

Consent Obligation – Disclosure of personal data without consent

Notification Obligation – Failure to notify individual of purposes for collection, use and disclosure of personal data

Purpose Limitation Obligation – Disclosure of personal data for purposes which have not been notified

11 June 2019

BACKGROUND

1 The organisation is a karaoke television (“KTV”) bar located in Boat Quay (“Organisation”). The central issue in this case is whether the Organisation had valid consent from its patrons to disclose their images recorded on closed-circuit camera footage (“CCTV Footage”). The disclosure was on a screen in a publicly accessible area of its premises.

2 Following an investigation into the matter, I found the Organisation in breach of s 13(a) read with s 18 and with s 20(1) of the Personal Data Protection Act 2012¹ (“PDPA”).

MATERIAL FACTS

3 The Organisation had one KTV room (“KTV Room”) on its premises. The KTV Room had a sign beside the TV screen which read: “Smile you are being recorded”. Patrons using the KTV Room were then

1 Act 26 of 2012.

recorded on CCTV Footage streamed “live” onto a screen in the Organisation’s public lounge (“Public Screen”) for general viewing.

4 On or before 19 June 2018, the complainant (“Complainant”) and her friends used the KTV Room and their images were live-streamed onto the Public Screen. After the Complainant and her friends left, the CCTV in the KTV Room malfunctioned. With the live streaming disrupted, the Organisation played on the Public Screen randomly selected recorded CCTV Footage. This included CCTV Footage of the Complainant and her friends which was replayed on the Public Screen for “a day or two”. After the Complainant found out about the replaying of the CCTV Footage, she lodged a complaint with the Personal Data Protection Commission (“PDPC”) on 19 June 2018.

FINDINGS AND BASIS FOR DETERMINATION

5 The provisions relevant to this case are as follows:

- (a) Section 13(a) of the PDPA states that organisations are prohibited from collecting, using or disclosing an individual’s personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data (the “Consent Obligation”).
- (b) Section 18 of the PDPA states that an organisation may collect, use or disclose personal data about an individual only for purposes (i) that a reasonable person would consider appropriate in the circumstances; and (ii) that the individual has been informed of under s 20, if applicable (the “Purpose Limitation Obligation”).
- (c) Section 20(1) of the PDPA states that an organisation is required to notify individuals of the purpose(s) for which it intends to collect, use or disclose an individual’s personal data on or before such collection, use or disclosure of the personal data (the “Notification Obligation”).

Personal data

6 The images of the Complainant and her friends on the CCTV Footage were their personal data as defined in s 2(1) of the PDPA. This was

regardless of whether the images were streamed live or replayed. The personal data was in the Organisation's possession and/or under its control.

The Organisation failed to obtain valid consent to replay the CCTV Footage with the personal data of the Complainant and her friends on the Public Screen

7 Upon review of the collected evidence, patrons were given notice that their images would be recorded and streamed live onto the Public Screen. First, they would have walked past the Public Screen before entering the KTV Room. In this regard, they would have noticed the Public Screen showing images of the KTV Room. Second, the sign beside the TV screen mentioned also notified the customers that they were being recorded.

8 However, there was no notice to the Complainant and her friends that their images could be randomly selected and replayed on the Public Screen when they were no longer in the Organisation's premises. The Organisation gave no notice to its patrons of the purpose(s) for which their recorded images would have been used. The only purpose evident from the circumstances was the live streaming visible to the patrons on the Public Screen. There was no evidence that a replay of CCTV Footage on the Public Screen was regular. Neither could it be said that replaying images of patrons in the KTV Room was an obvious response to CCTV malfunction, such that a reasonable person would have considered it natural and therefore appropriate. Music videos, for example, could have been screened.

9 Given the foregoing, as the Organisation had not notified the Complainant of the purposes for which the CCTV Footage would be reused, it follows that it had not obtained consent for the use and disclosure of the Complainant's personal data under s 13 read with ss 14(1) and 20(1) of the PDPA. On the facts, none of the other provisions in the PDPA would apply to allow the Organisation to replay the CCTV Footage on the Public Screen. In addition, the failure to notify the Complainant meant that the Organisation was not permitted to use and disclose the CCTV Footage in the manner which it did under s 18 of the PDPA. I therefore find that the Organisation had contravened ss 13 and 18 of the PDPA.

Remedial action

10 The Organisation did take remedial action. It ceased screening of CCTV Footage on the Public Screen. It improved its notification by informing patrons that CCTV recording is ongoing in its premises for security purposes.

CONCLUSION

11 Having found the Organisation to be in breach as above, I am empowered under s 29 of the PDPA to give the Organisation such directions as deemed fit to ensure compliance with the PDPA.

12 In determining the appropriate directions to be imposed on the Organisation, I have taken into account the following mitigating factors:

- (a) There was no evidence of any unauthorised use of the CCTV Footage of the Complainant and her friends other than the replay mentioned.
- (b) The Organisation did not receive any other complaints on this incident other than from the Complainant.
- (c) The Organisation was co-operative in the course of investigation.
- (d) The Organisation took prompt remedial action after being notified by the Complainant and PDPC.

13 Having considered all the relevant factors of the case, I have decided to issue a warning to the Organisation for breaching its obligations under s 13(a) read with s 18 and with s 20(1) of the PDPA, as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Grabcar Pte Ltd

[2020] PDP Digest 252

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1702-B0508 and DP-1703-B0613

Decision Citation: [2020] PDP Digest 252; [2019] SGPDPDC 14

Personal or domestic capacity

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

11 June 2019

INTRODUCTION AND FACTS OF THE CASES

1 This decision addresses, in the main, the obligations of an online ride-sharing platform and drivers who use the platform to provide carpool rides to passengers. Grabcar Pte Ltd (the “Organisation”) operates an online platform through the Grab mobile application (the “Grab App”) which enables individuals to book taxis or private cars for transportation services. The Grab App also provides a carpooling option, referred to in the app as “GrabHitch”. GrabHitch matches a passenger with a driver who is willing to give a lift to the passenger on the way to the driver’s destination in return for a fee. The Organisation states on its website:¹ “GrabHitch is a social carpooling platform powered by everyday, non-commercial drivers giving you a lift along the way to cover petrol costs.”²

2 This decision relates to separate complaints by two passengers (the “Complainants”) who used GrabHitch to book carpool rides. The carpool rides were provided by two different drivers (the “Drivers”) on

1 <www.grab.com/sg/hitch/>.

2 The Organisation’s website also states that GrabHitch is provided in compliance with the Road Traffic (Car Pools) (Exemption) Order 2015 (S 94/2015).

separate occasions. Nevertheless, the two complaints are dealt with together in this decision as they both relate to similar issues, in particular, to the issue of disclosure of passengers' personal data without consent by GrabHitch drivers.

3 The substance of each complaint was, in essence, that the Complainant's personal data had been disclosed without consent on social media by the Driver who gave a ride to the Complainant. The details of the complaints are summarised below:

- (a) The first complaint alleged that the Driver involved had posted various data relating to the first Complainant on a public Facebook Group named "GrabHitch Singapore Community" ("GHSC"). These data included screenshots of messages between the Driver and the Complainant which had been sent through the Grab App and a type-written post by the Driver which set out details of a dispute between the Driver and the Complainant and which identified the Complainant by name. The dispute in this case related to whether the Complainant should contribute to the payment of ERP charges and investigations revealed the reason that the Driver had made the posting was to seek views from other carpool drivers on how best to handle disputes relating to ERP charges.
- (b) The second complaint alleged that the Driver involved had posted various data relating to the second Complainant on a closed Facebook Group named "Uber/Grab SG Partners" ("UGSGP"). These data included (i) screenshots of messages between the Driver and the Complainant which had been sent through the Grab App and which included the Complainant's mobile phone number; (ii) screenshots of the Grab App which showed the name of the Complainant and the Complainant's pick-up and destination points; (iii) a screenshot of the Complainant's Facebook page which included her photograph, name and workplace; (iv) a typed-out post by the Driver which detailed his dispute with the Complainant and disclosed the Complainant's pick-up and destination points; and (v) a partial screenshot of SMS messages sent between the Driver and the Complainant, which included the Complainant's mobile number. The Driver's post in this case was about his dispute with the second Complainant on the payment of GrabHitch

charges. It appeared that the Complainant had insisted that she pay for the ride by card through the Grab App although the app indicated that the complainant was to pay for her ride in cash. Investigations revealed that the reason that the Driver had posted the above information was because the Organisation could not contact the Complainant to inform her of the situation and because the Driver was of the view that this was a case of non-payment.

4 Investigations also revealed that similar postings had also been made by other drivers on GHSC. Generally, these postings disclosed information such as passengers' names, photographs, ride details and the details of disputes between the drivers and their passengers.

5 The Organisation did not create or operate either the GHSC or UGSGP Facebook pages and investigations did not reveal any apparent link between the persons operating those pages and the Organisation.

ISSUES ARISING

6 Under s 13 of the Personal Data Protection Act 2012³ (the "PDPA"), organisations are prohibited from collecting, using or disclosing personal data about an individual unless the individual's consent is obtained, or collection, use or disclosure without consent is authorised or required under the PDPA or any other written law.

7 In addition, under s 24 of the PDPA, organisations are required to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised disclosure and various other listed risks.

8 In the circumstances, two main issues arise:

- (a) whether the Drivers are "organisations" under the PDPA, and if so, whether they had contravened s 13 of the PDPA in relation to the disclosure of the Complainants' personal data on the GHSC and UGSGP Facebook pages; and

3 Act 26 of 2012.

- (b) whether the Organisation had contravened s 24 of the PDPA with respect to the protection of the Complainants' personal data.

First issue – Are the Drivers “organisations” under the Personal Data Protection Act 2012?

GrabHitch drivers provide carpool rides in a personal capacity

9 The PDPA applies to organisations as defined under the PDPA. It is clear from the definition of “organisation” in s 2 of the PDPA that an individual may be an “organisation” for the purposes of the PDPA. However, s 4(1) of the PDPA further provides that Pts III to VI of the PDPA (which includes s 13) do not impose any obligations on any individual acting in a personal or domestic capacity.

10 GrabHitch drivers provide carpool rides on a non-commercial and non-profit basis in accordance with the Road Traffic (Car Pools) (Exemption) Order 2015⁴ (the “Exemption Order”) and as such are not required to obtain a private hire car driver’s vocational licence. In this regard, s 3(1) of the said Exemption Order states that:

Subject to sub-paragraph (2), the provisions specified in the Schedule do not apply to a person who uses a private motor car for the carriage of a passenger for hire or reward in the case where —

- (a) the person does not solicit for the passenger on a road or at a parking place or a public stand;
- (b) the carriage of the passenger is incidental to the person’s use of the private motor car;
- (c) the person informs the passenger, before the start of the carriage, of the person’s destination;
- (d) the person agrees with the passenger, before the start of the carriage, on the date of, pick-up and drop-off points of, and the payment (whether in cash or in kind) for, the carriage;
- (e) the amount or the value of any benefit in kind that the person collects from the passenger as payment does not exceed the cost and expenses incurred for the carriage of the passenger;

4 S 94/2015.

- (f) if there is more than one passenger, the aggregate of the amount or the value of any benefit in kind that the person collects from each of the passengers as payment does not exceed the cost and expenses incurred for the carriage of all the passengers; and
- (g) there is nothing in or on the private motor car displaying or referring to the fares for hiring the private motor car.

11 Consistent with this, the Organisation has a driver's code of conduct for GrabHitch drivers (the "Code of Conduct") which sets out the terms on which a GrabHitch driver may offer carpool rides. The Code of Conduct provides that:

Specific for carpooling, as mandated by the Law:

- (i) The motor vehicle used must be registered and insured in the name of the Driver and used by the Driver or any person by the Driver's authority expressly provided to the Company, the insurer of the vehicle and the relevant authorities
- (ii) The motor vehicle must not be used for the carriage of goods other than samples, any instructional purposes for reward, or the carriage of passengers for hire or reward purposes. These mean the Driver must:
 - Not solicit for passengers on a road or parking place or public stand
 - Ensure the carriage of the passenger is incidental to the Driver's use of his vehicle
 - Inform the passenger before the start of the carriage, of the Driver's destination
 - Agree with the passenger, before the start of the ride, on the date, pick-up and drop-off points, and the payment (whether in cash or in kind) for, the carriage
 - Ensure that the amount or the value of any benefit in kind that the Driver collects from the passenger as payment does not exceed the cost and expenses incurred for the carriage of the passenger
 - Ensure that if there is more than one passenger, the aggregate of the amount or the value of any benefit in kind that the person collects from each passenger as payment does not exceed the cost and expenses incurred for the carriage of all the passengers; and
 - Ensure that there is nothing in or on the motor vehicle that displays or refers to the fares for the hiring of the motor vehicle
 - Not exceed the local limit (if available) of car pool trips in each day on any motor vehicle

12 GrabHitch drivers agree to the Code of Conduct by virtue of their agreement with the Organisation as set out in the “Terms and Conditions for Singapore GrabHitch Drivers” (the “GrabHitch Terms”). In particular, in agreeing to the GrabHitch Terms, GrabHitch drivers agree that they “have read, understood, accepted and agreed with [the GrabHitch Terms], the conditions set out in the Driver’s Registration Form and the Driver’s Code of Conduct”.

13 In respect of the limit on carpooling trips that may be offered by a GrabHitch driver, the Organisation indicates the following in the “Frequently Asked Questions” (“FAQ”) section of its website:

How many trips can I offer a day as a Hitch driver?

Based on current carpooling regulations, non-commercial drivers can only complete 2 trips in a calendar day. While we appreciate your enthusiasm for carpooling, please note that 2 trips a day limit is set by LTA regardless of whichever platform you use.

We hope that you won’t put yourself and your riders at risk as your insurance may not cover if you do more than 2 trips a day in total, combined across all platforms.

For drivers who are worried their insurance does not cover GrabHitch rides, remember we are the ONLY carpooling service who has purchased additional insurance for extra coverage provided no regulations are breached.

14 Based on the foregoing, I find that GrabHitch drivers provide carpool rides in their personal capacity. This is especially so given that GrabHitch drivers:

- (a) are not allowed to solicit for passengers on the road, parking places or public stands;
- (b) are to ensure that their carrying of a passenger is merely incidental to their use of the vehicle;
- (c) can only collect payment for the trip on the basis of a recovery of costs and expenses for each trip; and
- (d) are only allowed to offer two carpool trips in each calendar day.

15 In the circumstances, GrabHitch drivers who are providing carpool rides in accordance with the applicable terms and conditions (as detailed above) are not subject to the PDPA. Accordingly, the Drivers cannot be in breach of s 13 the PDPA. It goes without saying that had any of the Drivers exceeded the daily limit of two carpooling trips, they would not be considered to have provided the carpool rides in a personal capacity.

Second issue – Did the Organisation contravene section 24 of the Personal Data Protection Act 2012?

16 Although the Organisation itself had not disclosed the Complainant's personal data, the Organisation is also required to put in place reasonable security arrangements to protect the personal data of passengers using the Grab App. In this regard, personal data obtained through the Grab App would be in the possession or under the control of the Organisation. This includes personal data such as the name and mobile phone number of the Complainant and any other information which was associated with, and related to, the Complainant, such as the Complainant's pick-up point and destination. However, personal data from the second Complainant's Facebook page would not be regarded as being in the possession or under the control of the Organisation.

17 In relation to the protection of passengers' personal data from unauthorised disclosure to third parties, the Organisation sets out the following in the Code of Conduct:

You are prohibited from posting passenger details in public forums including social media sites or sharing contact details. This is a violation of the Personal Data Protection Act.

18 This is the sole measure which the Organisation had put in place to prevent unauthorised disclosure of passengers' personal data on public forum sites which GrabHitch drivers may use. Investigations revealed that the two Drivers in question were unaware of the restriction in the Code of Conduct against posting passenger details on social media sites.

19 I find that merely including this restriction in the Code of Conduct is insufficient as a reasonable security arrangement to protect passengers' personal data. The Organisation makes its platform available to facilitate the hitching of rides or carpooling as part of its suite of commercial services. It has foreseen the risk that GrabHitch Drivers may post passenger details on social media sites as evidenced by its Code of Conduct. It could have done more to inform GrabHitch drivers of the range of acceptable and unacceptable conduct. However, apart from this entry in the Code of Conduct, there is nothing to indicate that this provision had been drawn to the attention of GrabHitch drivers or that they understood the importance of protecting passengers' personal data. Furthermore, as GrabHitch drivers are not subject to the PDPA, they may not be familiar with its provisions and the obligations imposed thereunder on organisations.

20 As has been held in *Re Habitat for Humanity Singapore Ltd*⁵ and *Re National University of Singapore*,⁶ reasonable security arrangements can include policies and practices as well as training. The Organisation ought to have put in place more detailed guidance for GrabHitch drivers to educate them about the need to handle the personal data of their riders, obtained through the Grab App, with care. As GrabHitch drivers are occasional drivers who may not be aware of the Organisation's obligations under the PDPA, the Organisation would have done well by introducing some form of online training for them. At the very least, the abovementioned restriction in the Code of Conduct could have been proactively highlighted to GrabHitch drivers. In its representations, the Organisation asserted that requiring it to train GrabHitch drivers would be onerous. This assertion was not substantiated and probably was premised on the assumption of a classroom-style training. Training is a means of communication and instruction that may take various forms and is one of the security arrangements that may be implemented by the Organisation to meet its obligations under the PDPA. It is ultimately up to the Organisation to determine the appropriate security arrangements it ought to implement to comply with its PDPA obligations. In the circumstances, I have acceded to the Organisation's request to amend the initial directions issued in the preliminary grounds of decision to remove the direction to train GrabHitch Drivers and instead leave it to the Organisation to ensure that it implements reasonable security arrangements to prevent the misuse and unauthorised disclosure of passengers' personal data.

REPRESENTATIONS MADE BY THE ORGANISATION

21 The Organisation has made representations dated 21 November 2018 in respect of the Commission's preliminary findings, asserting that it should not be found in breach of s 24 of the PDPA. Its central argument is that a GrabHitch driver does not drive in a "personal or domestic" capacity and should be considered an "organisation" that is required to comply with the PDPA in his own right. In support of this assertion the Organisation has highlighted the following factors:

5 [2019] PDP Digest 200.

6 [2018] PDP Digest 155.

- (a) By driving individuals who are not friends or family, the GrabHitch driver's activities move out of the private sphere and into the public. Accordingly, GrabHitch drivers are not driving in a "personal or domestic" capacity.
- (b) GrabHitch drivers "maintain independence" from the Organisation in deciding on the precise details involved in the provision of GrabHitch services (*eg*, how often they drive, where to go, how much payment to collect). GrabHitch drivers therefore "determine the purposes and means of processing the personal data" of the passengers, which is a defining characteristic of an organisation.

22 As a preliminary point, I would highlight that the Organisation's obligation under s 24 to protect personal data in its possession or control remains whether or not GrabHitch drivers drive in a personal or domestic capacity or in a capacity as organisations as defined under the PDPA. As such, the position adopted by the Organisation that GrabHitch drivers are required to comply with the PDPA in their own right does not address the finding that the Organisation is in breach of its obligation to protect personal data under s 24 of the PDPA.

23 It bears further repetition that in my view, the Organisation's measure of merely stating in its driver's Code of Conduct that GrabHitch drivers are prohibited from posting passenger details as set out at [17] above is insufficient to fulfil the Organisation's s 24 obligations, whether or not GrabHitch drivers are to be treated as organisations in their own right.

24 Turning to the specific positions taken by the Organisation as set out at [21] above, the first factor raised by the Organisation does not accord with the basic nature of the GrabHitch service, which is fundamentally a carpooling activity facilitated by the Grab App. Carpooling is a ride-sharing practice that private drivers engage in on a purely voluntary basis, and is best characterised as a social activity aimed at defraying the costs involved in owning and maintaining a private car and reducing road congestion. Human life is filled with interactions with people who are not friends or family, and it does not follow that the mere fact of interaction with strangers should elevate an act (in this case, carpooling) from the private to the public sphere.

25 In fact, the Organisation, in the FAQ material published on its own website,⁷ seems to recognise that GrabHitch drivers are engaged in an activity that is fundamentally private in nature:

Why should I sign up with GrabHitch? What's in it for me?

As a Hitch Driver, you get to benefit in 3 big ways: **Cover your petrol costs, make new friends and contribute to a car-lite Singapore! All these at your convenience!**

How is being a GrabHitch driver different from being a GrabCar driver?

They're not the same at all! **GrabCar drivers are commercial, professional drivers who have to register a business, purchase commercial insurance, convert their car to a commercial vehicle at the LTA and then sign up in person at the Grab office. Since Hitch Drivers are everyday, non-commercial private car owners who are not driving as a profession, the sign up process is way easier. No need for commercial vehicle conversion nor insurance, simply launch the Grab app, take a couple of photos and submit them for verification. And you're done!**

Am I still considered a Hitch Driver if I don't drive regularly?

Of course you are! **As a social initiative, we wouldn't want to stress you out by imposing any penalty for irregularity. So please go ahead and enjoy driving GrabHitch at your convenience!**

Why can't I get a GrabHitch driver as easily as GrabCar or GrabTaxi?

GrabHitch is meant as an advance booking service as **we are powered by non-commercial, everyday drivers who give Hitch Riders a lift at their convenience.** Hence, there may not always be any available Hitch Drivers who are heading the same way as you do at your specified time. To secure a higher chance of being matched, book as early as you could, even up to 7 days in advance!

What else should I take note of as a Hitch Rider?

1. **We are all about social carpooling and social carpooling is about being SOCIAL. Take the front seat and make new friends! Learn how to Hitch the right way here.**
2. **Your Hitch Driver is not a commercial driver like our GrabCar partners so they appreciate if you could treat them the same way you would treat a friend giving you a (discounted) lift to your destination!**
3. **Book in advance to maximise the chances of you getting a match! We can't emphasise this enough but really, it helps to be a little kiasu.**

⁷ Quoted portions retrieved from <<https://www.grab.com/sg/hitch/>> (accessed 10 December 2018).

Book the night before for a morning commute or 2 hours ahead of your evening ride home.”

[emphasis added in bold]

26 As repeatedly stressed in the Organisation’s materials quoted above, as compared to professional GrabCar drivers, the GrabHitch service is one that is non-commercial, only provided at the drivers’ own convenience, and primarily motivated by a desire to be social and to reduce the need for car usage. For all intents and purposes, a GrabHitch driver is no different from a driver offering a lift to a roadside hitchhiker out of goodwill. It is thus apparent from the published material that a GrabHitch driver engages in the activity in a purely personal capacity. It is also apparent, its present representations regarding this matter notwithstanding, that the Organisation recognises this. In fact, the private and casual nature of being a GrabHitch driver appears to be a main selling point for the Organisation.

27 In its representations, the Organisation also seeks to assert that whether the Land Transport Authority regulates GrabHitch drivers or not should be irrelevant to the determination of whether or not the drivers should be considered an organisation. The Organisation states that doing so will mean that only regulated or licensed individuals will be considered organisations. I think that this argument takes the logic too far. There is no intention to link the ambit of organisations under the PDPA to regulated activities. The interpretation that I have adopted is consistent with the scheme that exempts carpooling activities from the requirement of vocational licensing established under the Exemption Order. This is also consistent with how the Organisation has pitched GrabHitch through its FAQs and Code of Conduct for GrabHitch drivers as discussed at [11], [13] and [25] above.

28 It is not because of a supposed lack of regulation that the GrabHitch drivers are not considered organisations. Instead, it is precisely due to the personal and domestic nature of the activity they are engaging in that they are not subject to the same regulations as a commercial private hire car driver. If anything, the exemption of carpooling from the requirements of vocational licensing reflects the inherently private nature of carpooling (and by extension, the GrabHitch service). This is certainly reflected in the Exemption Order, which only applies to “private motor cars”. In addition, under s 3(1)(b) of the Exemption Order, “the carriage of the passenger *is incidental to* the person’s use of the private motor car” [emphasis added] –

unlike a taxi or private hire driver, the *raison d'être* of the GrabHitch driver is not the provision of transport; in other words, a GrabHitch driver is driving in a purely private capacity and the ferrying of a passenger in the context of a GrabHitch service is incidental to this private capacity.

29 The second factor raised by the Organisation relates to the “independence” of the GrabHitch drivers from the Organisation. The Organisation asserts that because a GrabHitch driver is able to decide when to provide GrabHitch rides, where to go, how payment is made and how much payment to collect, the Organisation has little control over the purposes and manner in which a GrabHitch driver processes personal data. Following from the above, the Organisation asserts that pursuant to the European Union General Data Protection Regulation, the drivers are “data controllers” who are able to “determine the purposes and means of the processing of personal data”.

30 The Organisation appears to have mistakenly equated the GrabHitch driver’s choice over whether to carpool with the control of purposes for, or the manner in, which personal data is collected, used or disclosed. In this regard, I note that the Grab App will automatically transmit the personal data (such as name and mobile number) of the GrabHitch passenger to the GrabHitch driver. This is how the Organisation programmed the Grab App to work – the GrabHitch drivers have no input in this collection and use of the personal data. In fact, it is the Organisation that discloses the passengers’ personal data to the GrabHitch drivers in the Organisation’s chosen manner and for the purposes the Organisation deems acceptable.

31 In the circumstances, the Organisation is in control of the personal data that it collects, uses and discloses when passengers wish to use the Organisation’s GrabHitch service. The “independence” of the GrabHitch driver as asserted by the Organisation is not the sole determinant as to whether he is an “organisation” under the PDPA. As I have concluded that the GrabHitch driver is not an “organisation” under the PDPA, it is unnecessary to delve into issues around joint controllership which may arise in respect of drivers for other services that the Organisation provides on its platform.

32 One final point bears highlighting. The activities of the GrabHitch driver are only made possible because of the Grab App. In providing the platform for private individuals (both drivers and passengers) to engage in the sharing economy, the Organisation bears responsibility for the personal

data that it collects from passengers and uses to provide its services, and discloses to GrabHitch drivers.

33 In the circumstances, and after considering the representations made by the Organisation, I find that the Organisation is in breach of s 24 of the PDPA.

DIRECTIONS TO THE ORGANISATION

34 Having found the Organisation to be in breach of s 24 of the PDPA, I am empowered under s 29 of the PDPA to give the Organisation such directions as I deem fit to ensure its compliance with the PDPA.

35 Taking into consideration the relevant facts in this matter, I hereby direct the Organisation to:

- (a) review and amend the Organisation's policies and practices to provide detailed guidance for GrabHitch drivers on the handling of the personal data of their riders and to communicate to GrabHitch drivers all relevant policies and practices (including the amended policies and practices) within 120 days of this decision to protect the personal data in the possession or control of the Organisation from unauthorised disclosure by GrabHitch drivers;
- (b) implement any other reasonable security arrangements as necessary to comply with s 24 of the PDPA; and
- (c) inform the Commission within seven days of the compliance with the above directions.

36 Given that only two individuals were directly affected by the unauthorised disclosure of personal data and in consideration of the type of personal data disclosed, I find that a financial penalty is not warranted in this matter.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Grabcar Pte Ltd

[2020] PDP Digest 265

Coram: Tan Kiat How, Commissioner

Case Number: DP-1801-B1526

Decision Citation: [2020] PDP Digest 265; [2019] SGPDPDC 15

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

11 June 2019

BACKGROUND

1 This case concerns the unauthorised disclosure of the names and mobile phone numbers of 120,747 GrabCar Pte Ltd (the “Organisation”) customers in marketing e-mails sent out by the Organisation (the “Incident”). On 5 January 2018, GrabTaxi Holdings Pte Ltd, a related corporation of the Organisation,¹ notified the Personal Data Protection Commission of the Incident on behalf of the Organisation. The Commissioner’s findings and grounds of decision based on the investigations carried out in this matter are set out below.

MATERIAL FACTS

2 The Organisation is part of the Grab Group, which offers, among other things, ride-hailing transport services, food delivery and payment services on its mobile platform. As part of its marketing strategy, the Organisation regularly conducts marketing campaigns to reach out to targeted customers. These frequently involve sending e-mails offering special promotions to selected customers.

1 The Legal and Compliance team for the Grab Group in Singapore sits within GrabTaxi Holdings Pte Ltd.

3 On 17 December 2017, the Organisation sent out 399,751 marketing e-mails to a targeted group of customers as part of a marketing campaign (“Marketing Campaign”). Out of the e-mails sent on that date, 120,747 e-mails contained the name and mobile phone number² of another customer, *ie*, the e-mail was sent to User A’s (the intended recipient) e-mail address but User B’s (the mismatched customer) name and mobile phone number was reflected in the e-mail as that of the intended recipient (the “Mismatched E-mails”).

4 Shortly after the Mismatched E-mails were sent out, the Organisation’s Customer Experience team reported an increased number of customer queries regarding the unauthorised disclosure of their personal data to other customers. The Organisation commenced investigations immediately thereafter. It determined that the Incident was caused by the erroneous assembly of customer information from different database tables that could, in turn, be traced to changes that had been made to the structure of its customer database since the previous marketing campaign.

5 The Organisation maintains a set of user attributes, *ie*, data points that describe every customer such as registration date, bookings and rides, in a database table (the “Main Table”). Each customer is assigned a unique “passengers_id” number in the Main Table. For the purpose of illustration, the Main Table would have appeared as follows:

passengers_id	name	passenger_email	passenger_mobile_no
12354567	Sally Goh	sal.g@amail.com	81456789
22558866	John Tan	jt@amail.com	84567894
76543211	Alex Lee	al@amail.com	91111212

6 On 24 November 2017, as part of the Organisation’s e-mail verification efforts,³ the Organisation’s Product Analytics team was instructed to add a new user attribute “is_email_verified”. The verified

-
- 2 A customer’s mobile phone number is linked to their account and a customer’s e-mail address could be linked to several mobile phone numbers. As such, the customer’s mobile phone number was included in the marketing e-mails to allow users to easily identify which of their accounts would be applicable for the promotion.
- 3 The e-mail verification exercise was undertaken to allow the Organisation to target customers with verified e-mail addresses for future marketing campaigns.

e-mail addresses were placed in a database table (the “Verified E-mail Database Table”) which was separate from the Main Table. Each customer in the Verified E-mail Database Table was assigned a unique “verified_email_user_id” number. For the purpose of illustration, the Verified E-mail Database Table would have appeared as follows:

verified_email_user_id	Name	verified_email
22558866	Luke Kang	Luke.k@amail.com
76543211	Mindy Ho	Mindy.ho@amail.com
12354567	M Hafiz	Hafizm@amail.com

In the above example, only Luke Kang, Mindy Ho and M Hafiz had verified their e-mails and would be included in the Verified E-mail Database Table. Those customers who did not verify their e-mails would not be included in the Verified E-mail Database Table.

7 The “passengers_ids” and “verified_email_user_ids” were created separately but both ID numbers are of the same integer length and comprise entirely of numerals (*ie*, without alphabets or other symbols). Unbeknownst to the Organisation at the time, some “verified_email_user_ids” were identical to some “passengers_ids” even though they did not identify the same customer.

8 At the time of the Incident, the procedure for using new user attributes to generate and send marketing e-mails was as follows:

- (a) Regional Marketing provides high-level marketing requirements.
- (b) Product Analytics creates the corresponding database queries (which were SQL commands), that identify and select the attributes to be used in the marketing campaign. This process is subject to some internal tests.
- (c) Data Engineering executes the database query to produce the data for the marketing campaign. The data file is then uploaded to an e-mailing system to generate the actual marketing e-mails for use in the campaign.
- (d) Regional Marketing “verifies” the final outcome by looking at the marketing e-mails that have already been sent out, typically by including some test account e-mail addresses in the e-mail blast.

9 In the present case, Product Analytics, who wrote the SQL command for the database query for the Marketing Campaign, wrongly equated

“verified_email_user_id” with “passengers_id” and treated them as the unique identifier for a customer. As a result of this error, the SQL command used “verified_email_user_ids” to select the attributes for producing the data to generate the campaign e-mails.

10 As a result, when the Data Engineering team used the SQL command to produce the data to generate marketing e-mails for the campaign, e-mail addresses were drawn from the Verified E-mail Database Table whereas the customer’s name and mobile phone number were drawn from the Main Table on the assumption that the “verified_email_user_id” and “passengers_id” referred to the same customer. The Mismatched E-mails were therefore created where the “verified_email_user_id” in the Verified E-mail Database Table coincided with another customer’s “passengers_id” in the Main Table. Using the sample information from the tables at [5] and [6] above, the consolidated table would have appeared as follows:

passengers_id	name	passenger_mobile_no	verified_email_user_id	verified_email
12354567	Sally Goh	81456789	12354567	Hafizm@amail.com
22558866	John Tan	84567894	22558866	Luke.k@amail.com
76543211	Alex Lee	91111212	76543211	Mindy.ho@amail.com

11 Using the above example, M Hafiz (who had verified his e-mail address) would have received an e-mail at his verified e-mail address, Hafizm@amail.com, with Sally Goh’s name and mobile phone number because the SQL command for the database query equated “verified_email_user_id” with “passengers_id” and his “verified_email_user_id” is identical to Sally Goh’s “passengers_id”. Similarly, Luke Kang (who had verified his e-mail address) would have received an e-mail at his verified e-mail address, Luke.k@amail.com, with John Tan’s name and mobile phone number as his “verified_email_user_id” is identical to John Tan’s “passengers_id”. Mindy Ho would have received an e-mail at her verified e-mail address, Mindy.ho@amail.com, with Alex Lee’s name and mobile phone number as her “verified_email_user_id” was identical to Alex Lee’s “passengers_id”.

12 Although a total of 399,751 marketing e-mails were generated and sent in the Marketing Campaign, only customers who had verified their e-mail addresses⁴ received the Mismatched E-mails as they were the only

4 The 120,747 affected individuals.

ones who were assigned a “verified_email_user_id”. E-mails were not sent to those who did not verify their e-mail addresses.

13 Following the Incident, the Organisation took the following remedial actions:

- (a) the Organisation implemented more rigorous data validation and checks to the addition/changing of user attributes process;
- (b) the Organisation changed its practices to require a third person to perform sanity checks of the data before triggering any new campaigns; and
- (c) the Organisation plans to incorporate privacy by design elements by masking mobile phone numbers (eg, 9*****11) in future marketing campaigns.

FINDINGS AND BASIS FOR DETERMINATION

14 The key issue for determination is whether the Organisation had complied with its obligations under s 24 of the Personal Data Protection Act 2012⁵ (“PDPA”).

15 As a preliminary point, customer names and mobile phone numbers are personal data as defined under s 2(1) of the PDPA as it is clearly possible to identify the individuals from that data. It was also not disputed that the personal data was disclosed mistakenly and without authorisation.

Whether the Organisation complied with its obligations under section 24 of the Personal Data Protection Act 2012

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

17 The Commissioner finds that the Organisation did not have adequate measures in place to detect whether the changes it made to the system that held personal data introduced errors that put the personal data it was

5 Act 26 of 2012.

processing at risk. As highlighted in *Re Flight Raja Travels Singapore Pte Ltd.*⁶

... [W]hen an organisation makes changes to a system that processes personal data in its possession or control, *the organisation has to make reasonable arrangements to prevent any compromise to personal data.* [emphasis added]

18 First, it is not disputed that the root cause of the Incident was an error with the database query command which erroneously treated the “verified_email_user_id” as the unique identifier when it joined data from two database tables. Essentially, the Organisation consolidated the Verified E-mail Database and the Main Table by equating the “verified_email_user_id” found in the Verified E-mail Database Table with the “passengers_id” found in the Main Table and running the command to extract the verified e-mail address of its clients from the Verified E-mail Database and the name and contact number of its clients from the Main Table. The result was that, where the “passengers_id” and the “verified_email_user_id” were coincidentally the same number, the command would have extracted the e-mail address corresponding to the “verified_email_user_id” of a client from the Verified E-mail Database and matched it with the name and mobile number corresponding to the “passengers_id” of a different client from the Main Table. Therefore, the first client would have been sent an e-mail from the Organisation with the name and mobile number of the second client.

19 Second, the Commissioner finds that the Incident arose in part because of administrative failures. In this regard, the Organisation itself admitted that the technical documentation for the new Verified E-mail Database Table was not sufficiently clear. If the documentation had been clearer, the employee who wrote the SQL command for the database query might not have made the erroneous assumption and would not have joined the two database tables in that way.

20 Finally, there were shortcomings in the way the Organisation conducted tests. Tests were conducted on non-verified e-mail addresses instead of on both non-verified and verified e-mail addresses. The core team of testers did not discover the mismatch between the customer’s e-mail address and his or her name and mobile number because the test

6 [2019] PDP Digest 243 at [8].

e-mail addresses used were not verified e-mail addresses and were therefore not affected by the erroneous joining.

21 There was another grave error in this case. Investigations disclosed that there had not been proper user acceptance testing of the SQL script before it was deployed into production. Product Analytics conducted technical tests, but Regional Marketing was not involved in user acceptance testing. The Regional Marketing team only verified the actual production run of e-mails, *ie*, e-mails that were already sent to customers. Hence, even if they detected any errors such as the mismatched data, it would have been too late to correct the error.

22 In the circumstances, the Commissioner finds that the Organisation had failed to make reasonable security arrangements to detect errors when preparing the change, *ie*, writing the database query, as well as in failing to conduct proper testing before implementing the change. It is therefore in breach of s 24 of the PDPA.

DIRECTIONS

23 Having found that the Organisation is in breach of the Protection Obligation under s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

24 In assessing the breach and determining the directions to be imposed, the Commissioner took into account the following mitigating factors:

- (a) the Organisation was co-operative during the investigation and in line with its implementation of its data breach management plan it notified the Commission voluntarily;
- (b) the Organisation took immediate effective remedial action in line with its implementation of its data breach management plan;
- (c) the personal data disclosed compromised only the individual's name and mobile phone number, which was not of a sensitive nature; and
- (d) the affected customer's personal data was only disclosed to one individual, *ie*, a customer whose "passengers_id" was identical to the affected customer's "verified_email_user_id" number.

25 The Organisation made representations to the Commission after the preliminary grounds of decision were issued and requested for a reduction in the financial penalty of \$16,000 provided in the said preliminary grounds of decision. The Organisation based this request on its prompt voluntary notification and implementation of a remediation plan, and the financial penalty amounts imposed in previous cases. In particular, the Organisation cited the cases of *Re Aviva Ltd*,⁷ *Re NTUC Income Insurance Co-operative Ltd*,⁸ *Re Flight Raja Travels Singapore*⁹ and *Re Challenger Technologies Limited*.¹⁰

26 The Organisation's voluntary notification and accountability practices had already been taken into account in assessing the financial penalty.

27 The cited cases are distinguishable from the present case. In *Re Aviva Ltd* and *Re NTUC Income Insurance Co-operative Ltd*, the financial penalty imposed was \$6,000 and \$10,000, respectively. The reason that this case warrants a higher financial penalty, even though it does not involve sensitive personal data (unlike in the previous two cases), is the much higher number of individuals affected. In this case, a total of 120,747 data subjects were affected, while only two data subjects were affected in *Re Aviva Ltd* and 214 data subjects were affected in *Re NTUC Income Insurance Co-operative Ltd*. Similarly, only 72 data subjects were affected in *Re Flight Raja Travels Singapore*.

28 *Re Challenger Technologies Limited* was one of the first grounds of decision which were issued. The Commission had taken into consideration the fact that the incident in that case happened in September 2014, only a few months after the coming into force of the PDPA, when organisations may not have understood fully the manner in which they were required to comply with their obligations. After more than four years since the PDPA has come into full force, this consideration is no longer applicable and organisations should not be referring to these early cases in estimating the quantum of the potential financial penalties that may be imposed.

29 The Commissioner hereby directs the Organisation to pay a financial penalty of \$16,000 in accordance with this direction, failing which,

7 [2018] PDP Digest 245.

8 [2019] PDP Digest 208.

9 [2019] PDP Digest 243.

10 [2017] PDP Digest 48.

interest, at the rate specified in the Rules of Court¹¹ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

11 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re DS Human Resource Pte Ltd

[2020] PDP Digest 274

Coram: Tan Kiat How, Commissioner

Case Number: DP-1802-B1756

Decision Citation: [2020] PDP Digest 274; [2019] SGPDPDC 16

Openness Obligation – Lack of data protection policies and practices

Protection Obligation – Unauthorised access to, and deletion of, personal data – Insufficient security arrangements

13 June 2019

BACKGROUND

1 Open source software is increasing in popularity and prevalence. This case illustrates the risks to companies in using default settings of open source software without any assessment of the security features. On 25 February 2018, DS Human Resource Pte Ltd (“DSHR”) informed the Personal Data Protection Commission (the “Commission”) of a data breach involving unauthorised access and deletion of its database by a hacker. Following an investigation into the matter, the Commissioner found DSHR in breach of ss 12 and 24 of the Personal Data Protection Act 2012¹ (“PDPA”).

MATERIAL FACTS

2 DSHR specialises in the outsourcing of part-time staff to the food and beverage industry in Singapore. Individuals interested in applying for a part-time job would enter their personal data into DSHR’s mobile application. The personal data collected by DSHR’s mobile application was

1 Act 26 of 2012.

stored on MongoDB database, an open source database software used by DSHR since April 2017 (“Database”).

3 The Database is hosted on the Amazon Web Services (“AWS”) server. The source code used by DSHR to perform specific functions on the Database was stored in Github, an online code repository. The administration of DSHR’s Database was handled mainly by DSHR’s director. At the material time, the Database stored personal data of approximately 2,100 individuals, including:

- (a) name;
 - (b) NRIC number;
 - (c) date of birth;
 - (d) gender;
 - (e) emergency contact;
 - (f) bank account details;
 - (g) work experience;
 - (h) educational qualification; and
 - (i) image of front and back of NRIC
- (collectively, “DSHR’s Data”).

4 On 24 February 2018, DSHR discovered unauthorised access to the Database and deletion of DSHR’s Data. The hacker demanded payment of 0.25 bitcoins in exchange for restoring the Database. Notwithstanding DSHR’s payment on the same day, the hacker did not restore the Database (collectively, the “Incident”). DSHR did not have a backup and was unable to recover the deleted DSHR’s Data.

5 DSHR took the following remedial actions after the Incident:

- (a) changed all of the passwords of its AWS account;
- (b) restricted connections to DSHR’s AWS server to DSHR’s IP addresses only;
- (c) disabled remote access to the MongoDB server software;
- (d) engaged consultants to perform vulnerability and penetration testing, and remedied the issues found in the tests, such as an issue concerning session management;
- (e) installed HTTPS at <www.dshradmin.com>;
- (f) changed the username of its AWS account; and
- (g) notified all affected individuals via SMS.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

6 It is not disputed that DSHR's Data is "personal data" as defined in s 2(1) of the PDPA. There is also no dispute that the PDPA applies to DSHR as it falls within the PDPA's definition of "organisation".

7 The issues to be determined by the Commissioner in this case are as follows:

- (a) whether DSHR had complied with its obligations under s 24 of the PDPA; and
- (b) whether DSHR had complied with its obligations under s 12 of the PDPA.

Whether DSHR complied with its obligations under section 24 of the Personal Data Protection Act 2012

8 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. It is not disputed that DSHR had possession and control of DSHR's Data stored in the Database, and hosted on the AWS server.

9 The investigations found that DSHR failed to put in place reasonable security arrangements to protect DSHR's Data for the following reasons:

- (a) The default settings of the MongoDB open source database software allowed remote connections through the Internet. By using the default settings, DSHR's Data stored on the Database was exposed. DSHR used the default settings without any assessment of whether this was a reasonable security arrangement to protect DSHR's Data stored on the Database. In this regard, DSHR admitted that it focused on the installation and functional use of the MongoDB database software rather than its security.
- (b) There was readily available information and documents on the security of the MongoDB software (*eg*, steps to take to enable access control and limit network exposure). This included MongoDB's blog post on 6 January 2017 referring to a "Security Manual and Checklist" which DSHR should have

referred to when installing the MongoDB software in April 2017. DSHR failed to do so. As highlighted in the Commission's *Guide to Securing Personal Data in Electronic Medium*, organisations need to put in place adequate protection for databases that contain personal data, and consider their security requirements when selecting a database product.²

- (c) DSHR's Data included bank account details which are personal data of a sensitive nature.³ As highlighted in *Re Credit Counselling Singapore*,⁴ 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 misuse or unauthorised use of such data. In the circumstances, it was completely inexcusable for DSHR to use the default settings in the MongoDB open source database software without addressing its mind to the questions whether remote access to DSHR's Data was necessary and, if not, ensuring that the remote access functionality of MongoDB was disabled.
- (d) More fundamentally, MongoDB did not have an administrator password by default. It is necessary for all organisations making use of IT solutions to secure the administrator account by changing its default password to something unique and not easily guessable.
- (e) The Commissioner finds that DSHR failed to put in place any security or access controls to the Database (*eg*, through password protection), resulting in DSHR's Data being exposed to the Internet. This case is analogous to the case *Re Propnex Realty Pte Ltd*,⁵ where it was found that the organisation failed to properly protect personal data as it did not have any security controls or restrictions (*ie*, proper authentication system) to prevent access from the Internet over the webpages that were stored on the server.

2 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* at paras 13.1–13.2.

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

4 [2018] PDP Digest 295 at [25].

5 [2017] PDP Digest 171.

10 The investigations also revealed that DSHR had inadequate patch management processes. At the material time, notwithstanding GitHub had published documentation on its website advising periodic manual review by users, DSHR relied completely on GitHub for MongoDB patch alerts. GitHub is a portal for collaborative storage and management of source code in the developer community. Its features include providing security alerts of common vulnerabilities. However, it is not a complete substitute for monitoring IT security portals (*eg*, common vulnerabilities and exposures system, or “CVE”) and the security and patch information feed direct from the software solution provider (*ie*, MongoDB). DSHR ought to have actively monitored for new patches released for software components and from the correct sources. Cyber attackers are well aware of vulnerabilities available for exploiting. It is important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities.⁶

Whether DSHR complied with its obligations under section 12 of the Personal Data Protection Act 2012

11 DSHR admitted that it did not have any policies or internal guidelines which specify the rules and procedures on the collection, use and disclosure of personal data. DSHR’s omission to do so and consequential failure to communicate such policies and internal guidelines to its employees amount to a breach of s 12 of the PDPA.

REPRESENTATIONS BY DSHR

12 In the course of settling this decision, DSHR made representations on the amount of financial penalty which the Commissioner intended to impose, while agreeing with the Commissioner’s findings and basis of determination set out above.

6 Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* at paras 16.3–16.4.

13 In its representations on the amount of financial penalty, DSHR requested that the Commissioner consider the following factors:

- (a) DSHR asserted that the Incident arose due to its director's negligence but hopes that the director's lack of technical knowledge may be taken into account;
- (b) the popularity of MongoDB database software and the fact that it was used by many big companies worldwide led DSHR's director to believe that the database would have reasonable security reliability; and
- (c) DSHR's determination to proceed with automation of its business processes notwithstanding difficulties faced, including hiring a full-time developer moving forward.

14 Having considered the representations, the Commissioner acknowledges DSHR's determination to automate its business processes and its director's initiative to do so in response to the Government's push for small and medium enterprises ("SMEs") to go digital, particularly when difficulties in hiring technically skilled staff would have discouraged others. The Commissioner would like to take this opportunity to highlight that good data management and protection practices need to be adopted from the onset of the digitalisation process, and these can be proportionate without being too costly. SMEs are urged to tap available government funding and support programmes to assist SMEs in their digitalisation efforts.

15 The Commissioner has decided to maintain the financial penalty set out at [19] below for the following reasons:

- (a) An organisation's lack of technical knowledge cannot be a mitigating factor. As explained in *Re WTS Automotive Services Pte Ltd*,⁷ the responsibilities of ownership do not require technical expertise. In this regard, if an organisation does not have the requisite level of technical expertise to manage its IT system, the organisation may either procure technical expertise internally (eg, by training its existing employees or hiring individuals with relevant expertise) or engage competent service providers and give proper instructions.

7 [2019] PDP Digest 317 at [24].

- (b) The security features or reliability of the MongoDB database software were not the issue. It was DSHR's failure to ensure that the appropriate security settings were configured to protect DSHR's Data. This is therefore not a mitigating factor.

THE COMMISSIONER'S DIRECTIONS

16 Given the Commissioner's findings that DSHR is in breach of ss 12 and 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue DSHR such directions as it deems fit to ensure compliance with the PDPA. This may include directing DSHR to pay a financial penalty of such amount not exceeding \$1m.

17 In assessing the breach and determining the directions, if any, to be imposed on DSHR in this case, the Commissioner took into account the following aggravating factors:

- (a) there was actual loss of DSHR's Data as the hacker managed to access and delete the entire Database;
- (b) there was also the risk of DSHR's Data being misused (*eg*, the front and back image of affected individuals' NRIC could be used to commit identity theft); and
- (c) DSHR's failure to password protect the Database was a serious lapse of a basic and integral IT security arrangement.

18 The Commissioner also took into account the following mitigating factors:

- (a) DSHR implemented reasonable corrective measures to address the technical flaws that resulted in the Incident. DSHR also notified all affected individuals via SMS.
- (b) DSHR co-operated with the investigations.

19 Having considered all the relevant factors of this case, the Commissioner hereby directs DSHR to pay a financial penalty of \$33,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court⁸ in respect of

8 Cap 322, R 5, 2014 Rev Ed.

judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re InfoCorp Technologies Pte Ltd

[2020] PDP Digest 282

Coram: Tan Kiat How, Commissioner

Case Number: DP-1802-B1674

Decision Citation: [2020] PDP Digest 282; [2019] SGPDPDC 17

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

20 June 2019

BACKGROUND

1 The case concerns the unauthorised access and disclosure of personal data arising from a registration exercise for a cryptocurrency initial coin offering (“ICO”). The Personal Data Protection Commission (“PDPC”) received six complaints on the matter on 5 February 2018. The organisation (“Organisation”) also notified the PDPC of the matter on the same day.

2 Following an investigation into the matter, the Commissioner found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ (“PDPA”). The Commissioner’s findings and grounds of decision of the matter are set out below.

MATERIAL FACTS

3 The Organisation had conducted a cryptocurrency ICO registration exercise via a website² (“Website”) which it owned and managed at the material time. The registration exercise was scheduled to take place between 5 and 26 February 2018.

1 Act 26 of 2012.

2 <<https://sentinel-chain.org/>> (accessed 4 May 2020).

4 The registration process involved two main parts:

- (a) Individuals (“Participants”) were asked to input name, e-mail address, date of birth, identification type and number, nationality, country of residence and residential address (“Personal Data Set”) on the registration page.
- (b) Participants also had to upload “Know-Your-Customer” (“KYC”) documents. A uniform resource locator (“URL”) would be assigned to a Participant after he or she had uploaded the KYC documents and clicked “Save”. The KYC documents included the following:
 - (i) an identification document with a photograph of the Participant;
 - (ii) documents showing proof of residence; and
 - (iii) a photograph of the Participant holding the identification document.

5 The incident was caused by a vulnerability in the design of the registration form. There was no requirement built into the system to authenticate the individuals downloading the KYC documents. The URL also contained a serialised file identity (“FileID”) as the last few characters of the URL in running numbers. The vulnerability allowed Participants assigned with a URL to access other Participants’ saved KYC documents by altering the last few characters of the assigned URL. The KYC documents of 21 Participants were downloaded by 15 other Participants via this vulnerability.

6 The Organisation took the server offline immediately after being informed by a Participant. The Organisation also contacted the 15 other Participants who had downloaded the KYC documents. They were told to destroy the KYC documents not belonging to them. This includes any personal data of other Participants that they may have retained.

7 Prior to the incident, the Organisation had engaged a vendor to design the registration form for the Website. Data protection elements were considered by the Organisation. The Personal Data Sets were to be encrypted and rendered inaccessible to third parties. Nonetheless, the same level of diligence with respect to the uploaded KYC documents was not exercised by the Organisation.

8 The Organisation conducted standard functional tests on the Website’s process and user flow prior to launching it. However, these did

not detect the vulnerability that caused the incident. The Organisation also did not conduct nor arrange for any penetration test or web application vulnerability scan.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

9 The issue for determination is whether the Organisation breached s 24 of the PDPA. 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.

10 The Organisation had full possession of and control over the personal data collected from the Participants. Although the Organisation had engaged a vendor to design the registration form, the vendor did not process any personal data on behalf of the Organisation. The Organisation managed the Website on its own. Thus, it retained full responsibility for the IT security of the Website and the personal data contained therein.

11 The Commissioner is satisfied that reasonable security arrangements had been made to protect the Personal Data Sets despite the vulnerability. Encryption of the Personal Data Sets had prevented unauthorised access by third parties.

12 However, insufficient protection was accorded to the KYC documents. The Organisation had only performed standard functional tests of the Website prior to launching it. No penetration test or web application vulnerability scan was conducted. Had these tests and scans been performed on the Website, the well-known vulnerability could be easily detected.

13 Given the type of personal data that the KYC documents contained, it is unreasonable that the Organisation had omitted the abovementioned security testing prior to the Website launch. The ease with which the vulnerability could be exploited via changing the last few numbers of the URL made this more egregious.

14 The Commissioner therefore finds the Organisation in breach of s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

15 Given 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 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.

16 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account the following mitigating factors:

- (a) The URL was only known to Participants at the material time and not to the public.
- (b) The KYC documents were downloaded by only a small number of Participants.
- (c) The exposure was for a very short time window of about 15 minutes.
- (d) The Organisation had taken immediate remedial actions to prevent further unauthorised access of the KYC documents.
- (e) The Organisation was co-operative during the investigation.
- (f) The Organisation had promptly notified the PDPC of the incident.

17 The Commissioner hereby directs the Organisation to pay a financial penalty of \$6,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court³ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

3 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Cigna Europe Insurance Company SA-NV

[2020] PDP Digest 286

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1806-B2241

Decision Citation: [2020] PDP Digest 286; [2019] SGPDPC 18

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

20 June 2019

BACKGROUND

1 Cigna Europe Insurance Company SA-NV is a company established in Belgium which offers health insurance solutions and coverage in Singapore through a registered branch office (the “Organisation”). On 1 June 2018, the Organisation notified the Personal Data Protection Commission (the “Commission”) of a data breach incident involving the inadvertent disclosure of certain personal data of individuals who had taken up health insurance coverage with the Organisation. The Commission commenced an investigation in order to determine whether the Organisation had failed to comply with its obligations under the Personal Data Protection Act 2012¹ (the “PDPA”).

MATERIAL FACTS

2 The Organisation provides health insurance coverage to employees of its clients and their families who decided to take up such coverage (“Members”). In order to provide this health insurance coverage, it collects, uses and processes personal data of the Members.

1 Act 26 of 2012.

3 In 2012, the Organisation entered into a services agreement (the “Services Agreement”) with Cigna European Services (UK) Limited (“CES”) for the provision of various insurance-related services. CES is a related company of the Organisation within the Cigna group of companies (“Cigna Group”). The services provided by CES included the processing of insurance claims (among other services) and this involved activities such as generating and sending claim settlement letters and letters accompanying cheque payments to Members who had made an insurance claim. Such claims were processed through an IT system which was operated by CES and used by various companies in the Cigna Group (the “System”). In order to make use of the System, the Organisation transferred its Members’ personal data to CES and these data were processed in the System.

4 It transpired that, in two separate incidents in January 2017 and May 2018, claims settlement letters intended for certain Members were erroneously sent by CES to other Members. These incidents were due to technical issues affecting the production of the claims settlement letters by CES. In the second incident, the technical issues also affected the production of payment accompanying letters which were sent to some Members. CES initially did not inform the Organisation about the first incident. The Organisation only came to know about the two incidents after the second incident occurred.

FINDINGS AND BASIS FOR DETERMINATION

5 The cause of the data breach incidents in this case may be traced to the technical issues in the System. As these matters were not within the Organisation’s operational control or even its knowledge prior to May 2018, the Organisation does not bear any direct responsibility under the PDPA for the occurrence of the two incidents.

6 Nevertheless, as the processing of the Members’ personal data by CES was pursuant to the Services Agreement between the Organisation and CES, the question arises as to whether the Organisation had in place the appropriate measures to ensure protection of the Members’ personal data while the data was stored with and processed by CES. In this regard, s 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, disclosure and similar risks.

7 I find that the Organisation had in place the appropriate measures or could rely upon measures established within the Cigna Group to ensure protection of personal data by CES and to monitor CES' compliance. These measures include the following:

- (a) The Organisation and CES had entered into the Services Agreement and an Interaffiliate Data Processing and Transfer Agreement in 2012 which required CES to protect personal data transferred to it by the Organisation. For example, various clauses in these agreements required CES:
 - (i) to protect the confidentiality of the Organisation's customer data;
 - (ii) to take appropriate and commercially reasonable measures to prevent, *inter alia*, unauthorised access or disclosure of such personal data and to ensure a level of security commensurate with the risks posed by the processing of personal data;
 - (iii) to comply with a specified set of security safeguards;
 - (iv) to notify the Organisation of any events that might impact the quality of CES' services and products;
 - (v) to give the Organisation access to the services for the purpose of reviewing and monitoring the quality of the services and the management of risks; and
 - (vi) to give the Organisation's internal and external auditors access to the services for the purpose of conducting audits.
- (b) There were various internal frameworks, policies and standards which apply to companies within the Cigna Group, including CES. These included, among others, the Cigna Information Protection ("CIP") and General Computing Control ("GCC") governance frameworks. These frameworks, policies and standards addressed various aspects of IT security (amongst other matters).
- (c) CES was subject to Cigna Group's corporate audit and annual GCC assessment processes which include security and data protection, as well as external audits which may include IT audit reviews.

8 Finally, as regards the causes of the two incidents, the Organisation has informed the Commission that the Cigna Group (including CES, the Organisation and other affected companies within the group) will be

improving its processes in order to prevent a recurrence of the incidents. The actions of CES that were directly related to the two incidents took place outside our jurisdiction and were not part of the Commission's present investigation.

APPLICATION OF SECTION 26(1) OF THE PERSONAL DATA PROTECTION ACT 2012 TO CROSS-BORDER DATA TRANSFERS

9 As this case concerns personal data which had been transferred from the Organisation (in Singapore) to CES (in the UK), another question which may arise is whether the transfer meets the requirements of the PDPA. Section 26(1) of the PDPA prohibits organisations from transferring personal data to a country or territory outside Singapore “except in accordance with requirements prescribed under [the PDPA] to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under [the PDPA]”. The relevant requirements are prescribed in Pt III of the Personal Data Protection Regulations 2014² (the “PDPR”). In particular:

- (a) Regulation 9(1) of the PDPR requires an organisation (referred to in the PDPR as a “transferring organisation”), before transferring personal data from Singapore to a country or territory outside Singapore, to “take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore ... is bound by legally enforceable obligations (in accordance with regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the [PDPA]”.
- (b) Regulation 10(1) provides that legally enforceable obligations (as referred to in reg 9(1)) include, among others, a contract in accordance with reg 10(2).
- (c) Regulation 10(2) provides that a contract referred to in reg 10(1) must:
 - (i) “require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the [PDPA]”; and

2 S 362/2014.

- (ii) “specify the countries and territories to which the personal data may be transferred under the contract”.

10 The effect of the statutory provisions cited in the preceding paragraph is that when a transferring organisation in Singapore and an overseas recipient enter into a contract governing the transfer of personal data from the transferring organisation to the recipient, that contract must meet the two requirements specified in reg 10(2) of the PDPR in order for the transferring organisation to have complied with s 26(1) of the PDPA. The second of these requirements (reproduced at [9(c)(ii)] above) is self-explanatory. In relation to the first requirement (reproduced at [9(c)(i)] above), the question is whether the contract requires the recipient to provide the appropriate standard of protection to the transferred personal data.

11 As stated in reg 10(2) (reproduced above), the standard of protection to the transferred personal data must be at least comparable to the protection under the PDPA. Determining the required standard for a particular contract would first involve considering how the PDPA applies to the personal data while it is in the possession or under the control of the transferring organisation (*ie*, before the transfer to the recipient). The contract should then be drafted to impose comparable obligations on the recipient in respect of the PDPA’s nine main data protection obligations.³ These obligations are:

- (a) the Openness Obligation (ss 11 and 12 of the PDPA);
- (b) the Consent Obligation (ss 13 to 17 of the PDPA);
- (c) the Purpose Limitation Obligation (s 18 of the PDPA);
- (d) the Notification Obligation (s 19 of the PDPA);
- (e) the Access and Correction Obligations (ss 21 and 22 of the PDPA);
- (f) the Accuracy Obligation (s 23 of the PDPA);
- (g) the Protection Obligation (s 24 of the PDPA);
- (h) the Retention Limitation Obligation (s 25 of the PDPA); and
- (i) the Transfer Limitation Obligation (s 26 of the PDPA).

3 As they are referred to in Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, in particular, at para 10.2 thereof.

12 As a general point, it is not necessary that a contract addresses all nine obligations. This would depend on factors such as the purpose of the transfer, the nature of the relationship between the transferring organisation and the recipient and the scope of data processing services which the recipient may be providing to the transferring organisation. For example, if the recipient will not be assisting the transferring organisation with the handling of access and correction requests in relation to the transferred personal data, it would not be necessary for the contract to address the requirements of ss 21 and 22 of the PDPA.

13 In the present case, the Protection Obligation (s 24) is relevant to the transfer of personal data from the Organisation to CES. As discussed in the preceding section of this decision, the Organisation had in place the appropriate security arrangements, including contractual provisions, which met the requirements of s 24 of the PDPA. Those contractual provisions would also meet the requirements of s 26(1) of the PDPA in relation to the Protection Obligation. (As an aside, this position would apply to other organisations in a similar relationship and similar circumstances, that is, where the recipient is a data intermediary of the transferring organisation and is processing personal data on behalf of and for the purposes of the transferring organisation.)

14 As the present case is concerned with the security arrangements put in place by the Organisation and the facts and circumstances of the case do not raise any particular concern as regards other aspects of the Organisation's transfer of personal data to CES, the Commission did not investigate further into the Organisation's compliance with s 26(1). I am satisfied that it is unnecessary to do so and hence make no finding in relation to that section.

CONCLUSION

15 In the light of the above, I find that the Organisation had not contravened its obligations under s 24 of the PDPA.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Xbot Pte Ltd

[2020] PDP Digest 292

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1803-1781

Decision Citation: [2020] PDP Digest 292; [2019] SGPDPDC 19

Openness Obligation – Lack of data protection policies and practices – Failure to appoint data protection officer

20 June 2019

INTRODUCTION

1 On 2 March 2018, the Personal Data Protection Commission (the “Commission”) received a complaint that Xbot Pte Ltd (the “Organisation”) had disclosed the personal data of property owners through the Strata.sg mobile application without their consent. The Commission commenced an investigation in order to determine whether the Organisation had failed to comply with its obligations under the Personal Data Protection Act 2012¹ (the “PDPA”).

MATERIAL FACTS

2 The Organisation developed and operated the Strata.sg mobile application (the “App”) and an associated website, <<http://Strata.sg>> (the “Website”), which provided access to a database of residential property transactions (the “Database”). The Database included information on transactions involving both private residential properties (“Private Properties”) and Housing Development Board (“HDB”) properties (“HDB Properties”). This information was made available to users of the App and Website and included a partial address (block number, road and, for HDB

1 Act 26 of 2012.

Properties only, a storey range), area, type and price for the properties listed. In addition, the complete addresses of the Private Properties (including the specific unit number) was made available to premium subscribers of the App or Website who paid a fee for access to the information in the Database.

3 The Organisation also collected personal data from users of the Website and users of the App in order to grant them access to the Database. The Organisation had a data protection policy for the Website (which it referred to as a “Privacy Policy”) but that policy did not mention or cover the personal data collected from users of the App. The App did not include any separate data protection policy nor any link to the Organisation’s data protection policy for the Website. In addition, the Organisation did not have any internal policies or procedures relating to its personal data practices. At the material time, the Organisation was run by a single individual who was also an employee of the Organisation. The Organisation had only one other employee.

FINDINGS AND BASIS FOR DETERMINATION

Does the information in the Database constitute personal data under the Personal Data Protection Act 2012?

4 Section 2(1) of the PDPA defines “personal data” 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 ...

5 The information in the Database would not, on its own, be personal data as none of those data could identify an individual (*per* limb (a) of the above definition). In particular, as there is no publicly available means of identifying the owners of the HDB Properties based on the information available in the Database, the information relating to HDB Properties would not constitute personal data under the PDPA.

6 However, the complete addresses of the Private Properties in the Database could be used to trace the names of the owners of those properties through the Singapore Land Authority’s Land Titles Register. The information in the Database could then be related to the identified or

identifiable owners of the Private Properties and reveal the type and size of property they own and the price they paid for the property. In the light of this, the information in the Database relating to Private Properties constitutes personal data under the PDPA (*per* limb (b) of the above definition).

Is the Organisation permitted to collect, use and disclose the personal data in the Database?

7 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing personal data about an individual for a purpose unless:

- (a) the individual consents, or is deemed to have consented, under the PDPA to such collection, use or disclosure; or
- (b) collection, use or disclosure without the individual's consent is permitted or required under the PDPA or any other written law.

8 In the course of the Commission's investigation, the Organisation admitted that it had not obtained the consent of the individuals concerned for the collection, use and disclosure of their personal data in the Database. Hence, the key issue is whether the Organisation is permitted to do so without the individuals' consent.

9 Under s 17(1) of the PDPA, collection of personal data without consent is permitted in the circumstances listed in the Second Schedule to the PDPA. In particular, para 1(c) of the Second Schedule permits the collection of personal data without consent if the personal data is publicly available. Section 2(1) of the PDPA defines the term "publicly available" (in relation to personal data) as "personal data that is generally available to the public". Use and disclosure of personal data which is publicly available is similarly permitted without consent under s 17(2) read with para 1(c) of the Third Schedule and s 17(3) read with para 1(d) of the Fourth Schedule, respectively.

10 In this case, the information in the Database had either been obtained by the Organisation from a source which was generally available to the public or had been derived by the Organisation from information which had been obtained from such a source. In particular, the Organisation had obtained information from the Urban Redevelopment Authority's Real Estate Information System ("REALIS") portal and the HDB's Resale Flat Prices portal. The information in these portals is available to members of

the public (in some cases, upon payment of a fee). In my view, such information is generally available to the public.

11 In the circumstances, I find that the Organisation is permitted under the PDPA to collect, use and disclose the personal data in the Database without consent of the relevant individuals. The Organisation is therefore not in breach of s 13 of the PDPA.

Did the Organisation have in place the necessary data protection policies and practices under the Personal Data Protection Act 2012?

12 Section 12 of the PDPA requires organisations to:

- (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA;
- (b) develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;
- (c) communicate to its staff information about the organisation's policies and practices referred to in para (a); and
- (d) make information available on request about:
 - (i) the policies and practices referred to in para (a); and
 - (ii) the complaint process referred to in para (b).

13 In this case, although the Website and the App collected the same personal data for the same purpose, the data protection policy published on the Website was expressly limited to personal data collected via the Website. This, in my view, is insufficient to meet the requirements of s 12 as users of the App would not have a clear indication of how their personal data would be handled by the Organisation. The Organisation should have ensured that its published data protection policy covered personal data regardless of whether it was collected via the Website or the App. This could have been done with some simple amendments to the current data protection policy and, as a good practice, the App could have included a link to the policy published on the Website. Alternatively, the Organisation could include a separate data protection policy within the App.

14 In addition to an organisation's published data protection policy, the "policies and practices" referred to in s 12 of the PDPA includes *internal* policies and processes that are necessary for the organisation to meet its obligations under the PDPA. While an organisation's published data

protection policy is meant to inform individuals about how their personal data will be handled by the organisation, the internal policies and practices are meant for the organisation's employees. Section 12 also requires such policies and practices to be communicated to the organisation's staff. These requirements are intended to ensure that all employees of the organisation are aware of the specific practices they must adhere to when handling personal data including, for example, the notifications to be given to individuals when their personal data is collected, how access and correction requests should be handled, how personal data must be kept and secured and how personal data must be disposed of when no longer required by the Organisation. The specific internal policies and practices which may be required for a particular organisation would depend on various factors such as the following (among other factors):

- (a) the type(s) and amount of personal data collected by the organisation;
- (b) the organisation's processes for collecting the personal data;
- (c) the organisation's purposes for using or disclosing the personal data; and
- (d) the number and roles of employees who require access to personal data in the course of their employment.

15 In the present case, the Organisation has one employee (in addition to the sole director). Nevertheless, it should have developed internal policies and practices, having in mind the considerations enumerated in the preceding paragraph, and communicated them to its employee so as to ensure that its employee adhered to the appropriate practices when handling personal data (and related matters) in the course of his or her employment. Although the Organisation is a small company, size of the organisation is but one determinant of the complexity of the internal policies and practices required. The types and amount of personal data that it possesses and controls is another relevant consideration. In this regard, the Organisation possesses and controls a not insignificant amount of personal data which relate to property ownership (even if these are publicly available).

16 In view of the above, I find the Organisation in breach of s 12 of the PDPA.

CONCLUSION

17 Having found the Organisation in breach of s 12 of the PDPA, I am empowered under s 29 of the PDPA to give to the Organisation such directions as I deem fit to ensure its compliance with the PDPA.

18 Taking the totality of the circumstances into account, I have decided to issue a warning to the Organisation for its breach of s 12 of the PDPA without further directions or imposing a financial penalty. In particular, I noted that:

- (a) the Organisation had ceased operations of both the App and the Website on 16 May 2018; and
- (b) the Organisation has been co-operative throughout the investigations.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re AIA Singapore Private Limited

[2020] PDP Digest 298

Coram: Tan Kiat How, Commissioner

Case Number: DP-1801-B1530

Decision Citation: [2020] PDP Digest 298; [2019] SGPDPDC 20

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

20 June 2019

BACKGROUND

1 On 5 January 2018, the organisation (“Organisation”) notified the Personal Data Protection Commission (the “Commission”) of the potential unauthorised disclosure (the “Incident”) of individuals’ personal data contained in 244 letters sent to two individuals due to an error with its letter generation system. In particular, 245 letters meant for various customers that the Organisation generated on 22 December 2017 and 27 December 2017 were sent to two customers as follows:

- (a) 179 letters were sent to the first customer (“Customer X”), of which 178 letters were received by him (with one having gone missing in transit); and
- (b) 66 letters were sent to, and received by, the second customer (“Customer Y”). Customer Y was the intended recipient of only one of these letters.

2 Following an investigation into the matter by the Commission, the Commissioner found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ (“PDPA”) for the reasons set out below.

1 Act 26 of 2012.

MATERIAL FACTS

3 The Incident arose from an error in the Organisation’s “Integral Life System” (the “System”) which was used to automatically generate certain types of letters to its customers. The error was introduced into the System as a result of the Organisation deploying a software fix (the “Fix”) on 21 December 2017 to rectify an earlier error (the “First System Error”). The First System Error resulted in the Organisation sending duplicate letters to customers who had provided the Organisation with only a foreign despatch address (*ie*, they had not provided any local despatch address in Singapore).

4 Unfortunately, the Fix inadvertently introduced a logic error² which caused the System to extract and reflect the wrong local despatch addresses on the affected letters. This logic error manifested itself when the System generated “HealthShield Non-Integrated for Foreigners Policy” letters (“Type A letter”) and letters which were not Type A letters (“non-Type A letter”) in a batch; the local despatch address of the non-Type A letters generated immediately after a Type A letter incorrectly reflected the local despatch address of that Type A letter (the “Error”). A more detailed description of this Error is provided below:

- (a) When the System generates Type A letters (*ie*, Letters 1 and 2 in Table 1 below), the Type A letters accurately reflect the local and/or foreign despatch address of the intended recipients.
- (b) If the System then generates non-Type A letters (*ie*, Letters 3, 4 and 5 in Table 1) immediately after a Type A letter, the non-Type A letters *wrongly* reflect the local despatch address of the *recipient of the last Type A letter* (*ie*, Letter 2 in Table 1), but accurately reflect their foreign despatch address (if any) (*eg*, Letters 4 and 5 in Table 1).
- (c) If the System generates Type A letters after a non-Type A letter (*ie*, Letter 6 in Table 1), the Type A letters accurately reflect the local and/or foreign despatch address of the intended recipients.

2 A logic error is a glitch in a computer program that causes it to operate incorrectly and produce unintended output or other behaviour, but not to crash.

5 Table 1 below illustrates the effects of the Error:

Table 1: Illustration of Error

Letter Number, in sequential order	Letter Type	System Policy Record		Despatch Address generated in the letters		Outcome
		Local Address	Foreign Address	Local Address	Foreign Address	
1	Type A	Tampines	-	Tampines	-	
2	Type A	Ang Mo Kio	India	Ang Mo Kio	India	
3	Non-Type A	Bedok	-	Ang Mo Kio	-	Letters 3 to 5 were sent to the local despatch address reflected in Letter 2 above.
4	Non-Type A	Ubi	USA	Ang Mo Kio	USA	
5	Non-Type A	-	Australia	Ang Mo Kio	Australia	
6	Type A	Eunos	-	Eunos	-	
7	Type A	East Coast	France	East Coast	France	
8	Type A	-	Vietnam	-	Vietnam	

6 In this case, the letters generated were therefore all addressed to their intended recipients, but 179 letters reflected the local despatch address of Customer X and 66 letters reflected the local despatch address of Customer Y. This is because Customers X and Y were in the position of the recipient of the last Type A letter (*eg*, Letter 2 in Table 1) before the batch of non-Type A letters was generated.

7 After the 245 letters were generated, they were converted into PDF format and sent to the Organisation's vendor, DataPost Pte Ltd ("DataPost"), for printing, enveloping and despatch. These letters comprised four Integrated Shield Plan premium notice reminder letters, 237 Integrated Shield Plan premium notice letters, three change of payor letters and one modified terms of coverage letter. These letters were sent to Customers X and Y between 28 December 2017 and 2 January 2018.

8 As a result of the Error, the following types of personal data for each category of letters were potentially compromised:

- (a) In respect of the modified terms of coverage letters, and Integrated Shield Plan premium notice letters and premium notice reminder letters:

- (i) the policyholder or insured person's full name;
 - (ii) the policyholder or insured person's policy number;
 - (iii) the policyholder or insured person's type and name of policy;
 - (iv) the policyholder or insured person's policy premium due date; and
 - (v) the policyholder or insured person's premium amount.
- (b) In respect of the change of payor letters:
- (i) the intended recipient's full name;
 - (ii) the intended recipient's policy number;
 - (iii) the intended recipient's type and name of policy;
 - (iv) the intended recipient's policy anniversary date;
 - (v) the insured person's full name, which differs from the intended recipient as the latter was paying the premiums on behalf of the insured; and
 - (vi) the intended recipient's premium amount.

9 On 30 December 2017, the Organisation learnt about the Incident from a social media post by Customer X and discovered the Error. It took the following remedial actions to mitigate the damage caused and to prevent the recurrence of similar incidents:

- (a) immediately implemented a software fix to resolve the Error in the System;
- (b) conducted and completed a scan of the System to check that all Singapore despatch addresses for letters sent to the Organisation's customers in 2017 were accurate;
- (c) implemented a function in the System to enable it to perform, and generate daily reports for the purposes of, the following:
 - (i) checking and validating that the despatch addresses printed on the automatically generated letters match the records of the intended recipients, as found in the System's database; and
 - (ii) flagging out non-conforming cases to automatically stop such letters from being transmitted to DataPost for printing;
- (d) took steps to retrieve the 244 letters which were sent to the wrong addresses and successfully retrieved 243 unopened letters. One letter was never received by Customer X and was determined to have been lost in transit; and

- (e) printed and re-sent the affected letters to the customers concerned and extended their deadline to respond to the matters contained therein.

FINDINGS AND BASIS FOR DETERMINATION

10 The main issue for determination is whether the Organisation breached s 24 of the PDPA. 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.

11 As a preliminary point, the Organisation had engaged DataPost to assist with the printing, enveloping and despatch of the letters on the Organisation's behalf. According to the agreement between the Organisation and DataPost, and as admitted by the Organisation in its responses to the Commission's queries, the scope of DataPost's engagement did not include checking the substantive contents of the letters it printed, enveloped and despatched on behalf of the Organisation; DataPost was only required to conduct sampling checks of the printouts in relation to the quality of presentation and alignment. Accordingly, the Incident did not relate to the scope of DataPost's engagement under its agreement with the Organisation.

12 Before examining the arrangements put in place by the Organisation, it should be noted that the personal data involved in this case includes insurance data, a category of personal data that is considered to be of a sensitive nature. It has been stated in previous decisions³ that personal data of a sensitive nature should be safeguarded by a higher level of protection. To reiterate *Re Aviva Ltd*:⁴

All forms or categories of personal data are not equal; organisations need to take into account the sensitivity of the personal data that they handle. In this

3 See, for example, *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 363, *Re NTUC Income Insurance Co-operative Ltd* [2019] PDP Digest 208, *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189, *Re Aviva Ltd* [2019] PDP Digest 145 and *Re Aviva Ltd* [2018] PDP Digest 245.

4 [2019] PDP Digest 145 at [17].

regard, the Commissioner repeats the explanation in *Re Aviva Ltd* [2017] (at [18]) on the higher standards of protection that should be implemented for sensitive personal data:

The Advisory Guidelines on Key Concepts in the PDPA states that an organisation should “implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity”. This means that *a higher standard of protection is required for more sensitive personal data. More sensitive personal data, such as insurance, medical and financial data, should be accorded a commensurate level of protection.* In addition, the Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data expressly states that documents that contain sensitive personal data should be “processed and sent with particular care”.

[emphasis added]

13 In this case, in order to determine whether the Organisation was in breach of s 24, the relevant question is whether it had put in place reasonable security arrangements that would have prevented the Incident. It appears from the Commission’s investigations that the Organisation had failed to:

- (a) conduct sufficient testing before rolling out the Fix for the First System Error; and
- (b) institute sufficient controls or checks to ensure the accuracy of the letters that the System automatically generated.

14 With respect to the failure set out above at [13(a)], the tests which the Organisation conducted after developing the Fix were limited to ensuring that the First System Error was addressed (*ie*, that duplicate letters were not sent to customers who had provided the Organisation with only a foreign despatch address). The scope of these tests was too narrow. Since changes were made to address how the System handled retrieval and insertion of local and foreign addresses, these tests should have been designed to ensure that the Fix did not affect other aspects of the System involving the same functionality.

15 Additionally, the tests were not conducted to mimic real-world usage of the System. Firstly, the Organisation conducted its tests by generating one letter at a time. However, the System was ordinarily required to generate letters in batches which included both Type A and non-Type A letters, and the Error in fact only arose when the letters were generated in such batches. If the Organisation had tested the batch processing

functionality using test data that approximated real-world scenarios, the Error would have likely come to light at that stage.

16 Secondly, the Organisation used a set of test data that was severely flawed. The test data used a single address, 1 Robinson Road, as the local despatch address for all the letters that were generated. The Organisation claimed to have done this in order to prevent the disclosure of production data. There are proven ways to generate dummy or test data that reflect the distribution of the production data without resorting to using a single address, *eg*, by swapping⁵ the data. Further, this measure would also have prevented them from detecting the Error even if they had tested the generation of letters in batches.

17 With respect to the failure set out above at [13(b)], the Organisation admitted that it did not have in place any process or personnel responsible for checking the contents of the automatically generated letters. The *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* states the following in relation to the use of automated processes:⁶

Ensure the accuracy and reliability of the automated processing implemented by checking these systems and processes regularly. When the data is more sensitive, consider incorporating additional checking mechanisms to cater for unexpected situations and ensure no error arises from the automated processing.

As good practice, establish procedures to include additional checks following the processing, printing and sorting of documents to ensure that the destination information (e.g. mailing address, email address or fax number) is correct and matches that of the intended recipient(s) prior to sending.

[emphasis added]

18 Given the sensitive nature of the personal data involved, the Organisation ought to have instituted controls or checks to ensure the

5 The purpose of swapping is to rearrange data in the dataset such that the individual attribute values are still represented in the dataset, but generally, do not correspond to the original records. This technique is also referred to as shuffling and permutation. For more details, please refer to Personal Data Protection Commission, *Guide to Basic Data Anonymisation Techniques* (25 January 2018).

6 Personal Data Protection Commission, *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* (20 January 2017) at para 2.1.

accuracy of the addressees of the letters. This is something that the Organisation has since implemented.

19 For the reasons above, the Commissioner found the Organisation in breach of s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

20 Having found that the Organisation is in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue the Organisation such directions as he deems fit to ensure compliance with the PDPA.

21 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the following mitigating factors were taken into consideration:

- (a) the Organisation voluntarily notified the Commission of the breach;
- (b) the Organisation fully co-operated with the Commission's investigations;
- (c) the Organisation took prompt action to mitigate the effects of the breach; and
- (d) the Organisation managed to retrieve 243 letters unopened.

22 In consideration of the relevant facts and circumstances of the present case, the Commissioner directs the Organisation to pay a financial penalty of \$10,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁷ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

23 The Commissioner has not made any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

⁷ Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re SME Motor Pte Ltd

[2020] PDP Digest 306

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1901-B3318

Decision Citation: [2020] PDP Digest 306; [2019] SGPDPDC 21

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

4 July 2019

BACKGROUND

1 On 31 January 2019, the Personal Data Protection Commission (the “Commission”) received a complaint from an individual (the “Complainant”) in relation to the disclosure of other individuals’ personal data that had been printed on the reverse side of an invoice issued to the Complainant by SME Motor Pte Ltd (the “Organisation”).

MATERIAL FACTS

2 The facts of this case and circumstances leading to the breach bear some resemblance to the cases of *Re SLF Green Maid Agency*¹ and *Re Furnituremart.sg*.²

3 The Organisation is in the business of auto repair and servicing. In an effort to be environmentally friendly, the Organisation had a practice of reusing scrap or unwanted paper documents by printing other documents on the reverse side.

1 [2019] PDP Digest 327.

2 [2018] PDP Digest 175.

4 The Complainant met with a car accident and brought her vehicle to the Organisation's workshop for repair. The Complainant subsequently discovered that the Organisation had printed her workshop repair invoice on a piece of paper that contained the personal data of two other individuals (the "Personal Data") on the reverse side. On 31 January 2019, the Complainant lodged a complaint with the Commission in relation to the disclosure of the Personal Data.

5 The Personal Data disclosed to the Complainant included the following:

- (a) the first individual's name, NRIC number and insurance policy number; and
- (b) the second individual's name, insurance policy number and claim number.

FINDINGS AND BASIS FOR DETERMINATION

6 The issue that arises in this case for determination is whether the Organisation had complied with its obligations under s 24 of the Personal Data Protection Act 2012³ ("PDPA"). 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.

7 As a preliminary point, the Organisation did not dispute that there was an unauthorised disclosure of the Personal Data. Having considered the material facts and circumstances, the Organisation did not have reasonable security measures in place to protect the Personal Data in its possession or under its control for the following reasons.

8 First, the Organisation failed to protect the Personal Data by not preventing the unwanted or scrap documents that contained personal data from being reused or given to other customers, and by not providing instructions on the proper handling and disposal of such documents. While the Organisation's internal guidelines ("Internal Guidelines") set out some minimal storage and disposal procedures for general documents, there was

3 Act 26 of 2012.

no mention of any process or system for segregating unwanted or scrap paper containing personal data from the pile of papers designated for reuse by the Organisation's employees. Given its silence on the practice of using the reverse side of documents containing personal data, I find that the Organisation's Internal Guidelines did not amount to an adequate security arrangement.

9 Second, the Organisation did not train its employees to be aware that customers' personal data could be at risk of unauthorised disclosure through the practice of reusing unwanted or scrap paper. During the investigation, the Organisation admitted that its employees used the reverse sides of unwanted documents for "environment protection" reasons. As noted in *Re SLF Green Maid Agency*,⁴ although the practice of reusing scrap or discarded paper is "highly commendable and environmentally-friendly ... organisations must take care to ensure that there is no personal data on the scrap or discarded paper set aside for such reuse". In this regard, the Organisation failed to show that it created employee awareness concerning the risk of unauthorised disclosure of personal data when reusing unwanted or scrap paper.

10 Third, the Organisation did not provide proper data protection training for its employees. It is well established that proper training is a key security arrangement in an organisation's compliance with the Protection Obligation.⁵ Proper staff training – which creates data protection awareness amongst employees, imparts good practices in handling personal data, and puts employees on the alert for threats to the security of personal data – is necessary to complement an organisation's data protection policies. Seeing as the Organisation regularly handles sensitive personal data such as NRIC numbers, insurance policy numbers and claims information, it is crucial for the Organisation to provide properly structured, periodic data protection training to its employees to help them identify risks and protect the personal data collected, used and disclosed in the course of their employment.

11 Taking all of the above into consideration, I find that the Organisation did not comply with its obligation under s 24 of the PDPA to

4 [2019] PDP Digest 327 at [1].

5 *Re National University of Singapore* [2018] PDP Digest 155 at [15]–[28]; *Re SLF Green Maid Agency* [2019] PDP Digest 327 at [12].

put in place reasonable security arrangements to protect the Personal Data in its possession or under its control.

REMEDIAL ACTIONS BY THE ORGANISATION

12 After being notified of the complaint on 26 February 2019, the Organisation undertook the following remedial actions:

- (a) implemented the following additional measures (“Additional Measures”):
 - (i) all documents containing personal data are no longer to be reused for printing;
 - (ii) the office manager to review documents at least once a week to ensure that (i) is complied with; and
- (b) instructed the data protection officer and officer manager to inform all employees of the Internal Guidelines and Additional Measures, and retrain them in this respect.

13 However, these Additional Measures failed to establish robust data protection policies and practices concerning the reuse and secure disposal of unwanted or scrap documents containing personal data, which would prevent the recurrence of another unauthorised disclosure of personal data or the occurrence of a similar data breach.

THE DEPUTY COMMISSIONER’S DIRECTIONS

14 Given my findings that the Organisation is in breach of s 24 of the PDPA, I am empowered under s 29 of the PDPA to issue the Organisation such directions as I deem fit to ensure compliance with the PDPA.

15 In assessing the breach, and determining the directions to be imposed, I took into account the following mitigating factors:

- (a) only two individuals were affected by the data breach;
- (b) the Personal Data was only disclosed to a single individual;
- (c) there was no evidence to suggest any actual loss or damage resulting from the data breach; and
- (d) the Organisation was co-operative during the investigations.

16 Having considered all the relevant factors of this case, I do not think that a financial penalty is warranted and instead make the following directions:

- (a) the Organisation is to comply with the provisions of the PDPA by putting in place a data protection policy and internal guidelines, which include a procedure for the proper control and disposal of unwanted or scrap documents containing personal data, within 30 days from the date of this decision;
- (b) the Organisation is to conduct training to ensure that its staff are aware of, and will comply with, the requirements of the PDPA when handling personal data within 60 days from the date of decision; and
- (c) the Organisation is to inform the Commission of the completion of each of the above directions within one week of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Spize Concepts Pte Ltd

[2020] PDP Digest 311

Coram: Tan Kiat How, Commissioner

Case Number: DP-1708-B1027

Decision Citation: [2020] PDP Digest 311; [2019] SGPDPDC 22

Openness Obligation – Failure to appoint data protection officer – Lack of data protection policies and practices – Failure to make information available on request about data protection policies and practices

Protection Obligation – Unauthorised disclosure of personal data – Insufficient security arrangements

Transfer Limitation Obligation – Failure to ascertain and ensure that recipient of personal data outside Singapore was bound by legally enforceable obligations to provide comparable standard of protection

4 July 2019

BACKGROUND

1 This complaint concerns an incident involving the personal data of customers of Spize Concepts Pte Ltd (“Spize”). Spize operates a chain of food and beverage outlets in Singapore. Part of its offering involves allowing customers to place orders through its online portal, <<https://orders.spize.sg>> (“Site”). The orders placed online will then be delivered to the customer at the stipulated address.

MATERIAL FACTS

2 On 12 August 2017, the Personal Data Protection Commission (“PDPC”) received a complaint from a member of the public regarding the Site. A link on the Site named “Call Center” (“Link”) had allowed members of the public to view three tabs: “Customer Ordering”, “Restaurants” and “Order Dashboard”. Under the “Order Dashboard” tab, approximately 148 customers’ personal data – specifically their names, contact numbers,

e-mail addresses and residential addresses (“personal data sets”) – were disclosed (“Incident”). The Incident was caused by a user logging into the managing director’s (“Managing Director”) administrator account to enable the Link to be publicly accessible on or around 9 February 2017. The Link was intended only for internal use and not accessible to the public.

3 Spize engaged Novadine, Inc (“Novadine”) to develop and host its Site and online ordering system in or around 2012. Personal data sets collected through the online ordering system were stored in databases within Novadine’s servers. Upon receiving news of the Incident on 14 August 2017, Spize requested Novadine to rectify the weakness in the Site. Novadine subsequently disabled the Link. The Link has not been publicly accessible since 16 August 2017.

FINDINGS AND BASIS FOR DETERMINATION

Issues for determination

- 4 The issues to be determined by the Commission are as follows:
- (a) whether Spize had breached s 24 of the Personal Data Protection Act 2012¹ (“PDPA”);
 - (b) whether Spize had breached s 11(3) of the PDPA by failing to designate an individual (“Data Protection Officer”) to be responsible for Spize’s compliance with the PDPA, and s 12(a) of the PDPA by failing to develop and implement policies and practices necessary to meet its obligations under the PDPA;
 - (c) whether Novadine was a data intermediary of Spize;
 - (d) whether Spize had breached s 12(d)(i) of the PDPA by failing to be in a position to make information available on request about its policies and practices which addressed the processing of personal data by Novadine on behalf of Spize; and
 - (e) whether Spize had transferred personal data outside of Singapore in breach of s 26 of the PDPA.

1 Act 26 of 2012.

Whether Spize had breached its obligation to protect personal data under section 24 of the Personal Data Protection Act 2012

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

6 Spize had outsourced the hosting, support and maintenance of its online ordering system to Novadine. However, that did not detract from its obligation under s 24 of the PDPA. In *Re Management Corporation Strata Title Plan No 3696*,² the PDPC had found that an organisation has the primary role and duty to protect personal data, even if the organisation had engaged another organisation (a data intermediary) to carry out the processing of personal data on its behalf.

7 Investigations revealed that Spize had failed to put in place or ensure the adoption of reasonable security arrangements to prevent data breaches such as the Incident from occurring.

8 First, Spize lacked knowledge of the Novadine system – in particular, knowledge that enabled the Link to disclose its customers’ personal data to the public. Based on Spize’s responses to the PDPC’s queries during investigations, it was apparent that Spize and its Managing Director, whose account was used to enable the Link, did not know about the existence of the Link or the consequences of enabling it.

9 Second, Spize lacked knowledge of the security arrangements that were in place within the Novadine system to protect personal data under its control that was being processed on its behalf. Spize had to rely on the answers provided by Novadine in describing how the Site and online ordering system worked. It was also unable to describe its arrangements with Novadine to process, protect and manage the personal data.

10 Spize’s lack of knowledge about how personal data was processed on its behalf by Novadine was caused and/or compounded by the lack of records in its possession. The employee previously responsible for documenting Spize’s arrangement with Novadine had since left Spize. Spize

2 [2018] PDP Digest 215.

also did not have any staff responsible to manage the relationship between Spize and Novadine.

11 The sum effect of the above is that Spize lacked knowledge of how the personal data that was being processed on its behalf by the Novadine system was protected.

12 Third, Spize's administrator accounts for the Novadine system, in particular the Managing Director's administrator account, lacked the necessary authentication and authorisation measures.

13 Spize mentioned that there was no password policy in place at the time of the Incident. Spize also acknowledged it did not set a mandatory password requirement when Novadine first created the accounts. The Managing Director's password was rudimentary and made up of eight digits. According to the PDPC's *Guide to Securing Personal Data in Electronic Medium*,³ there ought to be at least one alphabetical character and one numeric character for such passwords. Although the PDPC guide serves only to provide guidance, it is an indicator of how far short the password complexity and security was in this case.

14 Spize also did not mandate that its Managing Director's administrator account password be changed regularly. Nor did Spize monitor and/or ensure there was proper access to the Managing Director's administrator account. Indeed, Spize acknowledged that the account password was shared among several people at the material time, but could not provide details on the identity of these people and their respective designations.

15 The need for proper password management policies and regular change of passwords was made clear in the earlier decision of *Re Orchard Turn Developments Pte Ltd*.⁴ In that case, the PDPC had highlighted that an organisation's password management policies and practices, which include the regular change of passwords, formed an integral part of the security arrangements to protect personal data. Having failed to implement such proper password policies and practices, the PDPC had found the organisation in breach of s 24 of the PDPA.

16 Additionally, the improper handling and use of administrator accounts resulted in Spize not having control and not being able to monitor

3 Revised 20 January 2017.

4 [2018] PDP Digest 223.

which employees had access to the Managing Director's account. Consequently, when an unidentified party enabled the Link on 9 February 2017, Spize was unable to identify the employee responsible for doing so and discover the full facts surrounding the Incident.

17 In the light of the foregoing, Spize was found to have failed to make reasonable security arrangements to protect its customers' personal data under its control or in its possession. Accordingly, the Commissioner is satisfied that Spize was in breach of s 24 of the PDPA.

Whether Spize had breached the Openness Obligation sections 11(3) and 12(a) of the Personal Data Protection Act 2012

18 The PDPC's investigations revealed that Spize did not have any data protection policies, internal guidelines nor any accompanying terms and conditions in place at the material time. Spize also only appointed its Data Protection Officer on 21 August 2017, one week after the PDPC notified Spize of the weakness in its Site. In the light of these shortcomings, the Commissioner is satisfied that Spize had breached its Openness Obligation under ss 11(3) and 12(a) of the PDPA.

Whether Novadine was a data intermediary of Spize and whether Spize breached section 12(d)(i) of the Personal Data Protection Act 2012

19 An organisation has the same obligations as its data intermediary in respect of personal data processed on its behalf: see s 4(3) of the PDPA. In this regard, an organisation that engages a data intermediary to process personal data on its behalf would need to ensure that there are appropriate policies and practices in place (under s 12 of the PDPA) governing the data intermediary's processing of data. The question then is whether Novadine was a data intermediary of Spize and, if so, whether Spize has complied with s 12 of the PDPA in respect of personal data processed on its behalf.

20 Novadine has been in the business of providing software solutions for online food retail businesses since 2007. It is based in the US and offers its enterprise-class "Point-Of-Sale" integrated online ordering software to multi-unit restaurant chains. When orders are placed on the Site, Novadine processes such orders and hosts them on its servers. Novadine is therefore the provider of software-as-a-service, instead of an off-the-shelf software vendor.

21 Spize had been using the ordering system provided by and run by Novadine since 2012 to process online orders from its Singapore customers. During this process, Novadine collected and processed the personal data of Spize's customers in Singapore. Novadine collected the customers' personal data through an application designed, operated and maintained by Novadine through Spize's website. Spize's website and online ordering system were stored in Novadine's servers. Although Spize, when asked, could not produce any agreements or contracts with Novadine, on the totality of the documents produced by Spize, the Commissioner was satisfied that Novadine had processed personal data of Spize's customers.

22 Based on the above, the Commissioner is satisfied of the following. First, Novadine had processed personal data of Spize's customers in line with the arrangement stated above. Novadine was therefore Spize's data intermediary at the time of the Incident. Section 4(2) of the PDPA imposes on organisations that engage data intermediaries to do so "pursuant to a contract which is evidenced or made in writing". Spize was unable to provide documentary record to show that it had in place a contract with Novadine. The PDPC had made various requests for production of such documentation, but Spize was unable to produce information on its contract and/or arrangement with Novadine.

23 Second, Spize ought to have ensured that the policies and practices developed under s 12(a) of the PDPA addressed Novadine's processing of personal data on its behalf. Given that Novadine was Spize's data intermediary, Spize should also have had policies in place that addressed how Novadine processed personal data on Spize's behalf. As discussed in the preceding paragraph, one specific category of policies and practices is contractual documentation relating to the scope of the data intermediary relationship. Another is the category of policies and practices relating to the transfer of its clients' personal data outside Singapore that will be discussed in the next section.

24 Third, it follows that Spize was also in breach of its obligation under s 12(d)(i) of the PDPA to make information available on request about the policies and practices it had implemented, which addressed how Novadine was to process personal data on its behalf. Accordingly, Spize was in breach of s 12(d)(i) of the PDPA.

Whether Spize had transferred personal data outside Singapore in breach of section 26 of the Personal Data Protection Act 2012

25 Spize knew that Novadine was a software-as-a-service provider that was based in the US. It does not have any operations or other presence in Singapore. In choosing to use a data intermediary that is based outside Singapore, Spize had to ensure that Novadine was bound by legally enforceable obligations to protect personal data that it received to a standard comparable to that under the PDPA: reg 9(1)(b) of the Personal Data Protection Regulations 2014⁵ (“PDPR”). Pertinent to this case, Spize could have done so either by assessing that Novadine was subject to domestic laws in the US that provided comparative protection: reg 10(1)(a) of the PDPR; or through a contract: reg 10(1)(b) read with reg 10(2) of the PDPR. Alternatively, if Spize determined that the transfer came within one of the deeming provisions under reg 9(3) of the PDPR, then the assessment of comparable protection under US law or imposition of comparable protection through contract will not be necessary. The most pertinent exception in this case is reg 9(3)(b) of the PDPR, as the personal data of Spize customers was transferred to Novadine for the processing of their online food orders. As such, it could possibly be a transfer that is “necessary for the performance of a contract between the individual and the transferring organisation”: reg 9(3)(b) of the PDPR.

26 In the ordinary case, organisations are expected to make an assessment of the risks of transborder transfer of personal data in their possession or under their control and come to a conclusion as to how identified risks (if any) can be addressed. In this case, it is arguable whether the use of a US-based provider for an online ordering system was a question of necessity or a question of commercial choice. This makes a difference whether Spize can benefit from the deeming provision in reg 9(3)(b) of the PDPR, or whether it ought to have complied with reg 10 of the PDPR to ensure comparable protection by contract or through an assessment of US law.

27 The Organisation’s omission to consider its obligations under s 26 of the PDPA when transferring personal data outside Singapore constitutes a breach of the transfer limitation obligation under s 26. Assessments that US law provided comparative protection or that the transfer came within one

5 S 362/2014.

of the deeming provisions under reg 9(3) of the PDPR, *eg*, contractual necessity under reg 9(3)(b), should ordinarily be documented as part of the policies and practices that Spize ought to have developed and maintained. Alternatively, if transfer was on the basis of contract, clauses sufficient to meet the requirements of reg 10(1)(b) read with reg 10(2) of the PDPR should have been embodied in the contract between Spize and Novadine. The lack of policies and practices (including the lack of contractual documentation) evidencing the scope of Spize's engagement of Novadine is already the basis of a finding of breach of s 12(d)(i) of the PDPA.

DIRECTIONS

28 The Commissioner is empowered under s 29 of the PDPA to give the organisations such directions as it deems fit to ensure the organisations' compliance with the PDPA.

29 Having carefully considered all the relevant factors noted above, pursuant to s 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that:

- (a) Spize did not make reasonable security arrangements and is in breach of s 24 of the PDPA;
- (b) Spize breached its Openness Obligation under ss 11(3) and 12(a) of the PDPA;
- (c) Spize breached its obligation under s 12(d)(i) of the PDPA to make information available on request about the policies and practices it had implemented that would address how Novadine would process personal data on its behalf; and
- (d) Spize breached its obligation under s 26 of the PDPA.

30 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs that Spize pay a financial penalty of \$20,000 within 30 days from the date of the directions, failing which, interest shall be payable on the outstanding amount of such financial penalty.

31 In assessing the breach as determining the directions to be imposed on Spize in this case, the Commissioner took into account the fact that the Incident involved actual disclosure of customers' personal data through the Link via Spize's website.

32 That said, the Commissioner also took into account the following mitigating factors.

33 First, the Commissioner accepted Spize's representations that following the Incident, the organisation had taken steps to:

- (a) implement a customised data protection framework;
- (b) with help from external consultants, draft the necessary processes and policies and conduct data protection training for its employees;
- (c) engage a new IT vendor to change the Site (to be hosted locally) and online ordering system; and
- (d) put in place proper access controls within the system.

34 The Commissioner is satisfied that the above actions taken are reasonable and address the breaches that occurred in the present instance. They should also prevent recurrences of the Incident.

35 Second, Spize took prompt action to inform Novadine to remove the Link from the public domain.

36 Finally, Spize was largely co-operative during the investigations, notwithstanding its inability to explain the technical cause of the breach.

37 Spize, after receiving the preliminary decision, made the following representations in support of its request for a reduction in the quantum of the financial penalty imposed:

- (a) Spize reiterated the steps it had taken to comply with the PDPA after the Incident, namely,
 - (i) planning for an annual review of its data protection policy;
 - (ii) planning for retraining its current employees on the PDPA, in particular its IT team;
 - (iii) planning to send its employees for talks and seminars on PDPA updates;
 - (iv) initiating access-code restrictions as well as setting up separate accounts for employees; and
 - (v) terminating its engagement with Novadine and setting up a new website hosted by a company in Singapore;
- (b) the incident was unintentional and was a result of human error; and

- (c) the financial penalty is “a hefty price to pay” given a separate incident that Spize suffered last November (which was not related to personal data protection).

38 The Commissioner declines Spize’s request for a reduction in the quantum of the financial penalty for the following reasons:

- (a) the Commissioner had already taken into account the steps taken by Spize in reaching his decision on the quantum of the financial penalty (see [33] above);
- (b) the unintentional nature of the data breach is not relevant as a mitigating factor given that the investigations revealed that the breaches related to a failure to put in place the necessary processes and practices and did not relate to the specific action by the employee; and
- (c) an organisation which has difficulty in paying a financial penalty imposed may request that the financial penalty be paid in instalments. The fact that Spize suffered a separate incident is, however, not a relevant consideration in determining the quantum of the financial penalty imposed, although its impact on Spize’s cash flow may be a relevant factor to consider in a request for instalment payment of the financial penalty.

39 Further, the Commissioner hereby directs Spize to carry out the following within 60 days:

- (a) put in place a data protection policy and internal guidelines to comply with the provisions of the PDPA and, in particular, to prevent future recurrences of the breaches that had occurred in this case;
- (b) train all employees of Spize handling personal data on the obligations under the PDPA and the organisation’s data protection policies after direction (a) has been completed;
- (c) put in place proper access controls for the management of administrators’ accounts within its food order delivery and catering services website and online ordering system; and
- (d) put in place measures to ensure that it is able to make information available about its policies and practices (including information set out in contracts/agreements entered into with its data intermediaries that contractually require the relevant data

intermediary to implement specific reasonable arrangements) necessary to meet its obligations under the PDPA.

40 The Commissioner also directs that Spize inform the PDPC of the completion of each of the above within one week of implementation.

41 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 organisations will be taken.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re AgcDesign Pte Ltd

[2020] PDP Digest 322

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1805-B2072

Decision Citation: [2020] PDP Digest 322; [2019] SGPDPDC 23

Openness Obligation – Lack of data protection policies and practices – Failure to appoint data protection officer

4 July 2019

BACKGROUND AND MATERIAL FACTS

1 AgcDesign Pte Ltd (the “Organisation”) provides interior designing services for commercial and residential properties. Between 5 and 9 May 2018, the Personal Data Protection Commission (the “Commission”) received complaints alleging that the Organisation had used the complainants’ names and residential addresses without the complainants’ consent to send them marketing mailers. In the course of investigations by the Commission, it was found that the Organisation had sent the mailers using information from a database of property-related information obtained from a third party. That database had been compiled from information on caveats lodged with the Singapore Land Authority, which was publicly available.

2 It also emerged in the course of investigations that the Organisation had not appointed any data protection officer (“DPO”) and it had not developed and put in place any data protection policies. Upon being notified of the complaints, the Organisation appointed a DPO and issued certain verbal instructions to its employees concerning the collection, use and disclosure of personal data.

FINDINGS AND BASIS FOR DETERMINATION

3 Section 17 of the Personal Data Protection Act 2012¹ (“PDPA”), read with the relevant provisions of the Second, Third and Fourth Schedules to the PDPA, permits organisations to collect, use and disclose personal data which is publicly available without the consent of the individuals concerned. The Commission therefore did not proceed further with its investigation into the Organisation’s use of personal data in this case and I am satisfied that it is unnecessary to do so.

4 In relation to the Organisation’s failures to appoint a DPO and develop and implement any data protection policy, these are required under ss 11(3) and 12, respectively, of the PDPA. In particular, s 11(3) requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. Section 12 of the PDPA requires organisations to (among other things):

- (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; and
- (b) communicate information about such policies to its staff.

5 The importance of these requirements has been emphasised multiple times in previous decisions. For example, it is important for an organisation to document its data protection policies and practices in writing as they serve to increase awareness and ensure accountability of the organisation’s obligations under the PDPA.² Similarly, appointing a DPO is important in ensuring the proper implementation of an organisation’s data protection policies and practices, as well as compliance with the PDPA.³

6 In the circumstances, the Organisation was clearly in breach of ss 11(3) and 12 of the PDPA. While it has since appointed a DPO, it has not yet developed written policies and practices necessary to ensure its compliance with the PDPA.

1 Act 26 of 2012.

2 *Re Aviva Ltd* [2018] PDP Digest 245 at [32].

3 See, eg, *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [31]–[37].

THE DEPUTY COMMISSIONER'S DIRECTIONS

7 Having found the Organisation in breach of ss 11(3) and 12, I have decided to issue it the following directions under s 29 of the PDPA:

- (a) to develop and implement, within 30 days of the date of this direction, a data protection policy and the appropriate written internal policies and practices to comply with the provisions of the PDPA;
- (b) to communicate such policies and practices to its employees and conduct (or ensure that its employees attend) a suitable training course in order to ensure that employees handling personal data understand and comply with the requirements of the PDPA, both within 60 days of the date of this direction;
- (c) to inform the Commission of the completion of each of the above within seven days of completion; and
- (d) to pay a financial penalty of \$5,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁴ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

4 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re The Central Depository (Pte) Limited and another

[2020] PDP Digest 325

Coram: Tan Kiat How, Commissioner

Case Numbers: DP-1706-B0895 and DP-1705-B0908

Decision Citation: [2020] PDP Digest 325; [2019] SGPDPDC 24

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

22 July 2019

1 Organisations may employ vendors to carry out the printing and mailing of documents containing the personal data of their customers on their behalf. The process may involve both the organisations and vendors, which requires a concerted effort to protect personal data. This case presents the issue of division of responsibility in protecting personal data under the Personal Data Protection Act 2012¹ (“PDPA”) in such circumstances.

BACKGROUND AND MATERIAL FACTS

2 This case concerns the unauthorised disclosure of personal data of 1,358 account holders of the Central Depository (Pte) Limited (“CDP”) when their personal data was wrongly printed in the notification letters of other account holders and sent out. The incident occurred on or about 27 June 2017.

3 The exposed data included the name and/or CDP securities account number (“exposed primary identifiers”) which constitute personal data of the individual. In some notification letters, additional information on the securities owned by the individual (*eg.* name of security and total amount of dividends or distribution for the security) was also disclosed. These, when

1 Act 26 of 2012.

combined with the exposed primary identifiers, also constitute personal data of the individual.

Parties

4 CDP provides integrated clearing, settlement and depository facilities for customers in the Singapore securities market. Toppan Security Printing Pte Ltd (“TSP”) was engaged by CDP to carry out secure printing and dispatch of documents, including notification letters of CDP’s customers. Part of TSP’s engagement with CDP included developing the necessary bespoke software to print the relevant documents.

The printing process between CDP and TSP

5 There were three categories of notification letters to be printed depending on the type of investment(s) held by the account holder – (a) Distribution Reinvestment Plan – “DRP” or “D Type”; (b) Scrip Dividend Scheme – “SRP” or “S Type”; and (c) “Others” – “Others” or “O Type”. In this case, only the “DRP” or “D Type” notification letters are relevant because the data breach only affected this category of notification letters. Notification letters are sent to account holders to notify them of changes to and movements in their accounts.

6 During investigations, CDP and TSP represented to the Personal Data Protection Commission (“PDPC”) that the notification letters were printed in the following manner:

- (a) CDP sent the raw data in files over an encrypted channel to TSP. According to CDP, each file may have contained raw data for all three types of notification letters.
- (b) TSP decrypted the files for processing. The processing included the pre-processing, layout and printing stages.
- (c) The file provided by CDP contained the raw data in a plain text file. The data for a single account consisted of multiple lines. Each line comprised a label, which identified the type of data, and the corresponding data. To illustrate, a sample of the raw data would be supplied in the following manner:

D00001ABC	12345678X						
TRUST CO							
D000029876-54321-12346	MR ABC	123 DEF	DEF	654321	Y	SINGAPORE	
		ST	EST				
D00004Taxable	329862520						
Income							
D00004Tax Exempt	194494560						
Income							
D00004Capital	077797824						
D00004Other Gains	058348368						
D00005660503272							
D000029876-12345-64321	MS JKL	321 GHI		789456	Y	SINGAPORE	
		RD					
D00004Taxable	000001240						
Income							
D00004Tax Exempt	000000560						
Income							
D00004Capital	000000101						
D00004Other Gains	000000090						
D00005000001991							
D00001LMN	87654321X						
TRUST CO							
D000029876-00019-24689	MR QLM	98 WXY		987456	Y	SINGAPORE	
		ST					
D00004Taxable	000012541						
Income							
D00004Tax Exempt	000001560						
Income							
D00004Capital	000001201						
D00004Other Gains	000000290						
D00005000015592							

The raw data above is purely for illustrative purposes and the information is fictitious. As can be seen from the above table, the labels were designated “D00001”, “D00002”, “D00004” and “D00005”. For the lines with D00001, D00002 and D00005 labels, there was only one such line per account, while there could be more than just one line with D00004 labels for each account. The type of data that corresponds to each of the labels is as follows:

Label	Type of data
D00001	Name of the security.
D00002	Account number, account holder name and mailing address.
D00004	Information on credits to the account for the security. The data corresponding to the D00004 label can be further categorised into Taxable Income, Tax Exempt Income, Capital and Other Gains, such that there could be up to four lines with the D00004 label for each account.
D00005	Total value of the D00004 lines for each individual account.

At the pre-processing stage, TSP's program would carry out checks on the raw data to determine the integrity of the data and format the data into a consistent structure ("formatted data"), primarily to insert D00001 lines where multiple account holders have invested in the same security.

- (d) At the layout stage, a program extracts the formatted data and populates the data in each of the notification letters in the following layout:

Date _____ Securities Account Number: _____

Dear Sir/Madam

ABC Trust Co
Distribution Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on DD MM YYYY:

	Taxable Income*	Tax-Exempt Income	Capital	Other Gains	TOTAL
Unit(s)	A	B	C	D	X
Credited					

Please refer to the company's announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note

* Tax applied as per declaration form submitted by corporate account holders and is not applicable to individual holders.

(This is a computer generated advice and no signature is required.)

- (e) The final stage is the printing stage where the notification letters are printed as laid out and populated in the layout stage.

7 Before the deployment of the printing process, TSP had carried out user acceptance tests (“UAT”) on behalf of CDP, and the test results were presented to and approved by CDP.

The data breach incident

8 Prior to the data breach incident in June 2017, TSP had carried out successful print runs for S Type notification letters.

9 However, as indicated at [2] above, when the D Type notification letters were printed the first time, they were printed incorrectly. This occurred as the raw data only contained one D00004 line for some accounts instead of the four D00004 lines of data for which the layout stage of TSP’s system was programmed.

10 Where only one D00004 line was present, the notification letter should have appeared in a format similar to the following sample letter:

Date _____ Securities Account Number: _____

Dear Sir/Madam

ABC Trust Co
Distribution Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on DD MM YYYY:

Unit(s) Credited	Taxable Income* A	TOTAL X

⊗

Please refer to the company’s announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note
* Tax applied as per declaration form submitted by corporate account holders and is not applicable to individual holders.
(This is a computer generated advice and no signature is required.)

□

11 Instead each incorrectly printed notification letter included data which did not belong to that account. An example of a notification letter (using fictitious information) that was printed and sent out is as follows:

27 Jun 2017 Securities Account Number: 29876-54321-12346

Dear Sir/Madam

ABC TRUST CO

DISTRIBUTION Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on 27 Jun 2017

	TAXABLE INCOME*	0000003298625-20	LMN TRUST HOLDINGS	9876-00019-24689	TOTAL
Unit(s) Credited	329862520	0	27,082,017	SMITH, JOHN LIMITED	750

Please refer to the company announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note

* Tax applied as per declaration form submitted by corporate accountholders and is not applicable to individual holders.

(This is a computer generated advice and no signature is required.)

12 A comparison between the sample notification letter which was correctly printed as shown at [10] above and an example of the incorrectly printed letter shown at [11] above shows that the information marked out within the larger oval ought not to have been printed. The information in the third, fourth and fifth columns, which has been marked out, shows information relating to another individual, including his name (*ie*, John Smith), securities account number (*ie*, 9876-00019-24689) and the security invested in (*ie*, LMN Trust Holdings). The total marked out within the smaller oval is also incorrect.

13 The incorrectly printed notification letters resulted from the programming of TSP's system at the layout stage to expect exactly four lines of D00004 data for each account, instead of allowing it to accept up to a *maximum* of four lines of D00004 data. As will be discussed below, this was due to TSP misunderstanding each account to always consist of four D00004 lines (*ie*, the categories of Taxable Income, Tax Exempt Income,

Capital and Other Gains). However, in reality each account may consist of between one and four D00004 lines. The manner in which this error resulted in the incorrectly printed notification letters is described as follows:

- (a) Taking the below table of raw data as an example, at the layout stage, the program had correctly read the first and second lines, which had the D00001 and D00002 labels, respectively.

Line No.						
1	D00001ABC TRUST CO	12345678X				
2	D000029876-54321- 12346	MR ABC	123 DEF ST	654321	Y	Singapore
3	D00004Taxable Income	329862520				
4	D00005329862520					
5	D00001LMN TRUST CO	87654321X				
6	D000029876-00019- 24689	MR QLM	98 WXY ST	987456	Y	Singapore
7	D00004Taxable Income	000012541				
8	D00005000012541					

- (b) The program did the same for the third line which had a D00004 label (*ie*, for the Taxable Income category).
- (c) However, as the raw data did not include any D00004 lines for the “Tax Exempt Income”, “Capital” and “Other Gains” categories, the layout program instead assigned lines four (which was the total credits to the account), five (the name of the security for the next account) and six (the account holder name and residential address of the said next account) to these D00004 categories in respect of the first account.
- (d) The program then ignored the seventh line from the D00004 label of the next account.
- (e) Accordingly, when the printing was subsequently triggered, the notification letter that was printed had contained the data of the D00001, D00002 and D00004 labels from the next account. It also skipped the printing of the notification letter for that next account, since parts of the data had been merged with the current notification letter and the trailing data field was ignored.

- (f) This error was repeated for the other notification letters of the affected account holders.

14 Following the incident, CDP had issued apology letters to the affected account holders and halted its engagement with TSP in respect of its print services.

FINDINGS AND ASSESSMENT

Issues for determination

- 15 The issues to be determined by the Commissioner are as follows:
- (a) what obligations did CDP and TSP each owe under the PDPA in respect of the personal data of the affected account holders;
 - (b) whether CDP complied with its obligation under s 24 of the PDPA in respect of the data breach incident that occurred; and
 - (c) whether TSP complied with its obligation under s 24 of the PDPA in respect of the data breach incident that occurred.

CDP's and TSP's obligations to protect personal data under the Personal Data Protection Act 2012

Relevant provisions under the Personal Data Protection Act 2012

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

17 This obligation is also conferred on the data intermediary under s 4(2) of the PDPA. Further, s 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

18 The duties of an organisation and data intermediary under s 24 of the PDPA have been examined in precedents, *eg, Re Singapore Cricket Association*.² This case gives occasion to restate that duty.

Relationship between CDP and TSP in complying with section 24 of the Personal Data Protection Act 2012

19 In this case, CDP is the organisation and TSP is the data intermediary in respect of the personal data of the account holders. Both CDP and TSP are obliged under the PDPA to protect the personal data of account holders pursuant to s 24 of the PDPA as stated above.

20 The overlap in obligation for organisation and data intermediary to protect personal data means, in practical terms, that organisations and their data intermediaries would necessarily have to work together in formulating the right protective measures and processes.

21 This is especially pertinent in this case because both CDP and TSP had roles in developing the system or process by which the notification letters were printed. Amongst other things, CDP was the one which determined the format of the raw data and the specifications for which TSP would build its program around to generate the notification letters which required the processing of personal data and the printing and dispatch of those notification letters.

22 Hence, both CDP and TSP had the obligation to ensure that the printing system and process they developed would sufficiently protect the personal data it was handling and processing. As part of this, there needed to be proper testing of the system and implementation of exception handling and checks to prevent errors from compromising the security of the personal data. In the Commissioner's view, this responsibility fell on both CDP and TSP.

23 One of the ways in which organisations can develop a system which protects personal data is by adopting a "Data Protection by Design" approach in which organisations consider the protection of personal data from the earliest possible design stage of any project and throughout the project's operational lifestyle. This may be very relevant to organisations

2 [2019] PDP Digest 270.

which are looking to develop any new processes that deal with personal data (as in this case). This is a design approach that is advocated in the PDPC's *Guide to Developing a Data Protection Management Programme*.³

Whether CDP complied with its obligations under section 24 of the Personal Data Protection Act 2012

24 CDP's duty under s 24 was to make reasonable arrangements to protect the personal data to be processed on its behalf. As explained at [21] and [22] above, CDP had the responsibility in the development, testing and implementation of exception handling of the system to ensure that it would adequately protect personal data. In the Commissioner's view, this entails:

- (a) Providing clear specifications and representative test data that covered the full range of data to be processed and the various processing scenarios. Specific to the present context, this meant making clear that there was a range in the number of D00004 lines (*ie*, between one and four lines) per account in the data file supplied by CDP. In *Re Singapore Cricket Association*,⁴ the Deputy Commissioner had found that the provision of proper and clear instructions to a developer of a website that holds personal data should form part of the protection obligations of the organisation. In failing to do so, the Singapore Cricket Association was found in breach of s 24 of the PDPA. The same principles apply here.
- (b) Advising on the scope of the UAT since the test is based on test data provided by CDP. CDP would therefore need to supply test data that covered the full range of scenarios for processing in order for there to be proper UAT testing. Again, this included supplying test data that allowed for a range of D00004 lines to be tested.
- (c) Ensuring that the requirements that it provided anticipated and catered for processes that could handle exceptions and could verify that the processing was carried out correctly.

3 Published 1 November 2017, at para 4.4.1.

4 [2019] PDP Digest 270.

25 The Commissioner finds that CDP did not discharge its duty under s 24 of the PDPA:

- (a) CDP did not provide reasonably clear specifications to TSP. CDP knew that some of its D Type letters had just one D00004 line instead of four. However, the specifications that CDP provided to TSP did not make this clear:
 - (i) There was no explicit statement by CDP making clear to TSP that the number of D00004 lines may vary.
 - (ii) Instead, what was indicated in CDP's specification was that the D00004 lines were "repetitive". This could be understood to mean that there would be more than one D00004 line, and since CDP had only provided TSP with samples which had four D00004 lines at that stage, TSP misunderstood this to mean that they would always occur four times, *ie*, four D00004 lines for each notification letter. Had there been more clarity from CDP on what it meant at that point, the issue may have been averted.
- (b) CDP did not ensure that the UAT carried out was robust enough to test for variations in the number of D00004 lines that may be encountered in actual cases. This is because CDP had only supplied test data that had exactly four D00004 lines per account, for initial tests as well as UAT, and, as such, did not detect any problems with variations to the number of D00004 lines of data. The test data supplied also gave the mistaken impression that there were exactly four D00004 lines of data for each notification letter. A wider range of test data would have allowed for broader scoping of the UAT, which is lacking in this case.
- (c) CDP did not specify exceptional scenarios and how the printing system would handle exceptions or verify that processing was correct:
 - (i) As the organisation with primary and supervisory responsibility to protect personal data,⁵ CDP did not ensure that the printing system could detect and raise alerts when an exception or error was encountered.

5 See *Re Management Corporation Strata Title Plan No 3696* [2018] PDP Digest 215 and *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160.

- (ii) As will be examined below, TSP's layout program did not detect that there was only one line of D00004 data supplied in respect of some accounts, instead of the four D00004 lines it was hardcoded to read, and to trigger an alert. Instead, it continued to extract or ignore the subsequent lines erroneously. TSP's layout program had therefore lacked the capability to handle exceptions or issues arising from the data supplied.
- (iii) Additionally, CDP also did not satisfy itself during UAT that TSP's system had the means to verify that the data was processed correctly throughout all the stages of the process.

26 Having regard to the above, the Commissioner finds CDP to be in breach of s 24 of the PDPA.

Whether TSP complied with its obligations under section 24 of the Personal Data Protection Act 2012

27 The Commissioner likewise finds that TSP did not discharge its duty under s 24 of the PDPA. First, TSP ought to have ensured that the software it used correctly processed and printed out the relevant data. Giving TSP the benefit of the doubt and assuming that it had processed them correctly, TSP would have understood the requirements to mean that there were always four lines of D00004 data. TSP's layout program did not detect that in this case, there was only one line of D00004 data; and it went on to read the subsequent lines as though they were D00004 data. If the program was hardcoded correctly to expect four lines of D00004 data, it ought to have recognised that some accounts only contained one line of D00004 data and the system ought to have raised an alert in cases of deviation.

28 The program read the subsequent lines incorrectly as if they were D00004 data as the program did not check for four occurrences of D00004 labels per account but assumed that this was always the case. Thus, even based on TSP's misunderstanding that there will always be four D00004 lines per account, TSP's program was not designed to detect an exception to this (albeit mistakenly) expected feature. The incorrect processing of the data by TSP's program at the layout stage was what caused the notification letters to be printed and sent wrongly. There was a lack of exception and

error handling such that it cannot be said that TSP had implemented a reasonable security arrangement that would protect personal data.

29 The incident may have been prevented if the developers of the program had co-ordinated and adopted the same interpretation of the requirements. In this regard, TSP's program incorporated two checksum tests at the pre-processing stage. One checksum test was a check that the value of the D00005 data for each account correctly totalled the value of the D00004 lines for each account. The second checksum test calculated the total value of the D00005 data of all the accounts sent to TSP for printing. The pre-processing stage of TSP's system would then check if the data it received is accurate by comparing the total value of the D00005 data of all accounts CDP sent to TSP with the total value stored in the very last line of the file as a separate record. However, these checksum tests at the pre-processing stage were ineffective to address the unauthorised disclosure in this matter; it was merely a check on the integrity of the file received by TSP.

30 Ultimately, TSP did not implement the proper capability to detect or handle exceptions or errors in the processing and printing of the notification letters. It is fundamental to the protection of personal data that the system handling personal data is able to detect and carry out exception and error handling. Otherwise, this may lead to a system failure which poses risks of a data leak or data breach (as in this case).

31 It is timely for the Commissioner to refer to the PDPC's *Guide for Printing Processes for Organisations*,⁶ which states that organisations should consider the following, amongst other things, for their printing process:

Appropriate juncture for the check(s) i.e. performed at a suitable stage for corrective actions to be able to reverse and/or eliminate any potential error(s).

Intensity and extent of check(s) should be proportionate to the volume and sensitivity of the personal data present in the printing process.

32 TSP did not carry out a proper test on the system. It ought to have tested for variations in the number of D00004 lines that are provided to verify whether TSP's program is able to handle those variations such as different number of lines for the D00004 labels. These variations may

6 Published 3 May 2018, at p 6.

occur due to inadvertence or mistake, and TSP ought to test whether its program is able to handle them.

33 For the reasons above, the Commissioner finds TSP to be in breach of s 24 of the PDPA.

DIRECTIONS

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

35 Pursuant to s 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that CDP and TSP did not make reasonable security arrangements and are in breach of s 24 of the PDPA.

36 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs:

- (a) that CDP pay a financial penalty of \$24,000 within 30 days from the date of the directions, failing which, interest shall be payable on the outstanding amount of such financial penalty; and
- (b) that TSP pay a financial penalty of \$18,000 within 30 days from the date of the directions, failing which, interest shall be payable on the outstanding amount of such financial penalty.

37 In assessing the breach and determining the directions to be imposed on CDP in this case, the Commissioner took into account the following aggravating and mitigating factors:

- (a) CDP is the central depository for financial market account information in Singapore. Individual account holders must be able to rely on CDP to protect their personal data.
- (b) The personal data that was disclosed comprised of financial information of the individual, which is sensitive personal data.
- (c) That said, CDP took steps to prevent recurrence following the data breach incident.

- (d) CDP also promptly notified the affected individuals and the PDPC.

38 CDP submitted representations on the proposed decision in this case by way of a letter dated 8 April 2019. In its representations, CDP acknowledged that the specifications, test data and test scope provided to TSP could have been, and should be, improved. However, it was of the view that it had not breached s 24 of the PDPA.

39 In this regard, CDP asserts that TSP ought to have reviewed the specifications, test data and UAT for both the S Type and D type letters, instead of just the D Type letters, as the specifications for the print program would have been similar. According to CDP, it had provided an S Type letter template to TSP which consisted of a maximum of two D00004 lines and provided UAT test data for S Type letters which consisted of one D00004 line. CDP asserts that “[f]rom this TSP ought to have been aware that the actual data sent by CDP for printing may vary from the templates/test data provided”. Also, CDP asserts that it has specified in the specification that the number of the D00004 lines would be “repetitive”, *ie*, “not a fixed number of lines of crediting details but with variations within this type of crediting details”. Further, CDP asserts that it had used the word “always” to indicate if a value or the number of lines is fixed or static and it did not indicate that the number of D00004 lines “always” consisted of four lines.

40 The Commissioner agrees that TSP is also liable for unauthorised disclosure of personal data in the wrongly printed notification letters and has already found TSP to be in breach of s 24 of the PDPA. Nevertheless, CDP’s representations do not absolve CDP of its shortcomings in respect of this incident. CDP’s use of the word “repetitive” in its specifications was ambiguous when considered together with the fact that the test data provided to TSP for the D Type letters all contained four D00004 lines per account. This led TSP to assume that “repetitive” meant four D00004 lines for each account. It did not help that even though the test data provided had some records with four D00004 lines and others with fewer D00004 lines, the records with four D00004 lines were associated with D Type letters. Even though CDP intended for the dataset to be applicable for all types of letters, its omission to inform TSP led TSP to make the assumption that D Type letters always had four D00004 lines. CDP could have expressly instructed TSP that the test data provided was to be treated

as applying across all the various types of letters and not merely the individual types of letters to which the test data corresponded.

41 CDP also asserted that it had requested TSP to conduct an additional visual check on the notification letters, and that if TSP had done so, it would have caught the error. In relation to this, CDP referred to a “Document Management Services Agreement” (“DMSA”) entered into between CDP and TSP to support its assertion. However, a review of the DMSA does not reveal a specific requirement to conduct a visual check of the letters that are sent out. In the circumstances, the Commissioner did not accept CDP’s representations that it had instructed TSP to conduct a visual check of the notification letters.

42 Finally, CDP requested that, should the Commissioner maintain his finding that CDP was in breach of s 24 of the PDPA, the financial penalty imposed be reduced. In this regard, CDP made two submissions. First, CDP acknowledged that the disclosed personal data was sensitive but asserted that the potential harm to the affected individuals was relatively limited and not likely to lead to any loss or prejudice. The Commissioner agrees that there is no evidence of financial loss or damage. The absence of financial loss or damage has already been taken into consideration in determining the financial penalty imposed in this case.

43 Secondly, CDP also referred to its prompt notification of the error to affected individuals and to the PDPC, as well as to the proactive and prompt steps CDP took to remediate the matter. The Commissioner accepts these points and has included them at [37(d)] above.

44 In the circumstances, the Commissioner maintains his finding that CDP was in breach of s 24 of the PDPA. However, taking into account CDP’s representations, the Commissioner has decided to reduce the financial penalty from the initial quantum of \$30,000 to the amount stated at [36(a)] above.

45 In assessing the breach and determining the directions to be imposed on TSP in this case, the Commissioner took into account the following aggravating and mitigating factors:

- (a) The personal data that was disclosed comprised of financial information of the individual, which is sensitive personal data.
- (b) TSP was co-operative and willing to provide information on a timely basis to the Commission.

- (c) TSP took steps to prevent recurrence following the data breach incident.

46 The Commissioner hereby directs CDP to carry out the following within 60 days:

- (a) for CDP's data protection officer (appointed under s 11(3) of the PDPA) to be given authority to assess the data protection requirements in developing new printing processes that involve personal data; and
- (b) for CDP to provide the full range of expected processing scenarios in the test script during development testing and UAT for all types of printing jobs (except for *ad hoc* printing jobs) which are being carried out by TSP as at the date of this direction.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re ChampionTutor Inc

[2020] PDP Digest 342

Coram: Tan Kiat How, Commissioner

Case Number: DP-1710-B1269

Decision Citation: [2020] PDP Digest 342; [2019] SGPDPDC 25

Definition of business contact information

Openness Obligation – Failure to appoint data protection officer

Openness Obligation – Lack of data protection policies and practices

22 July 2019

BACKGROUND

1 On 31 October 2017, the Personal Data Protection Commission (the “Commission”) received a complaint from a former tutor (“Complainant”) who had registered with ChampionTutor Inc (“Organisation”), stating that he found a URL link¹ (“URL Link”) to the Organisation’s tutor list (“Tutor List”) through a Google search (the “Incident”). The Commission proceeded to investigate the Incident in order to determine whether the Organisation had complied with its obligations under the Personal Data Protection Act 2012² (“PDPA”).

MATERIAL FACTS

2 The Organisation is a home tuition agency in Singapore with more than ten years’ experience matching students and tutors. While the service is free for students, tutors are required to pay a commission to the Organisation for each tuition assignment they accepted.

1 <https://www.championtutor.com/certs_tutor/1certs1397642794.pdf>.

2 Act 26 of 2012.

3 In the course of investigations by the Commission, it was found that the Tutor List contained the name, contact number and e-mail address (“Disclosed Information”) of a total of 4,899 individuals, including the Complainant (“Affected Individuals”).

4 It also emerged in the course of investigations that the Organisation had not appointed any data protection officer (“DPO”) and had failed to develop and put in place any internal data protection policies.

FINDINGS AND BASIS FOR DETERMINATION

5 The issues to be determined by the Commissioner in this case are as follows:

- (a) whether the Disclosed Information is “business contact information” as defined under s 2(1) of the PDPA; and
- (b) whether the Organisation had complied with the obligations to appoint a DPO and develop and implement data protection policies and practices under ss 11(3) and 12, respectively, of the PDPA.

Whether the Disclosed Information is “business contact information”

6 Under s 2(1) of the PDPA, “business contact information” is defined as “an individual’s name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his *personal purposes*” [emphasis added]. Section 4(5) of the PDPA provides that the substantive data protection obligations found in Pts III to VI of the PDPA (the “Data Protection Provisions”) shall not apply to business contact information (“BCI”).

7 The purpose for which the contact information is provided is key to determining whether it is considered BCI. In this regard, the Affected Individuals provided the Disclosed Information to the Organisation for the purposes of being contacted for tuition assignments.

8 Under s 2(1) of the PDPA, “business” is defined as including “the activity of any organisation, whether or not carried on for the 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”. Tutors carry out a business of providing tuition services. In this regard, the tutors registered with the Organisation are freelancers, and are paid directly by the student. For each tuition assignment accepted, tutors are required to pay the Organisation a one-time commission.³ Tutors are also responsible for reporting their earnings as a freelance tutor to the tax authority yearly.⁴ The Inland Revenue Authority of Singapore’s *Tax Guide for Tuition Industry* provides guidance for tutors providing tuition services and tuition agencies assigning tutors to students with respect to reporting business income for tax purposes.⁵

9 Based on the foregoing, the Commissioner finds that the tuition services offered by the Organisation’s tutors fall within the definition of “business” under s 2(1) of the PDPA. Therefore, the contact details provided by the Affected Individuals for the purpose of being contacted for tuition assignments are BCI, and the Data Protection Provisions do not apply.

Whether ChampionTutor complied with its obligations under sections 11 and 12 of the Personal Data Protection Act 2012

10 The Organisation’s admission that it had not appointed a DPO at the material time is a breach of s 11(3) of the PDPA. In this regard, s 11(3) requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. The importance of appointing a DPO in ensuring the proper implementation of an organisation’s data protection policies and practices, as well as compliance with the PDPA, was emphasised in *Re M Stars Movers & Logistics Specialist Pte Ltd.*⁶

3 See “FAQ” *Champion Tutor* <<https://www.championtutor.com/faq.html>> (accessed 26 March 2020) which provides that agency commission is calculated at 50% of the first payment cycle (four weeks).

4 See “FAQ” *Champion Tutor* <<https://www.championtutor.com/faq.html>> (accessed 26 March 2020).

5 See Inland Revenue Authority of Singapore, “Tax Guide for Tuition Industry” (26 September 2017).

6 [2018] PDP Digest 259 at [31]–[37].

11 Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to communicate information about such policies and practices to its employees (among other obligations).

12 At the material time, the Organisation had a privacy policy to inform tutors and students about how it collects, use, disclose, manage and safeguard personal information provided by them in the course of accessing and using the Organisation's website.

13 The Organisation did not employ full-time staff but employed part-time home-based tuition co-ordinators to liaise with tutors and students, process e-invoices and follow up on payment. These part-time co-ordinators had access to personal data of the tutors and students in the course of their work. However, the Organisation did not have any internal data protection policies which specify the rules and procedures on the collection, use and disclosure of personal data. This omission meant that part-time tuition co-ordinators were not provided with any form of guidance with the PDPA and amounts to a breach of s 12 of the PDPA. An organisation that relies wholly on part-time staff needs to pay especial attention to ensuring that its policies can be easily accessible and that it has an effective system for promoting awareness and training part-time staff on its data protection policies and practices.

THE COMMISSIONER'S DIRECTIONS

14 Given the Commissioner's findings that the Organisation is in breach of ss 11(3) and 12 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding \$1m.

15 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account as a mitigating factor that the Organisation had co-operated with investigations and was forthcoming in its response.

16 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to do the following:

- (a) pay a financial penalty of \$5,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court⁷ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full; and
- (b) within 60 days from the date of the Commissioner's directions, develop and implement an internal data protection policy and appoint a DPO.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

⁷ Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Genki Sushi Singapore Pte Ltd

[2020] PDP Digest 347

Coram: Tan Kiat How, Commissioner

Case Number: DP-1809-B2684

Decision Citation: [2020] PDP Digest 347; [2019] SGPDPDC 26

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

Personal Obligation – Higher standard of protection needed to protect sensitive personal data

22 July 2019

BACKGROUND

1 On 7 September 2018, Genki Sushi Singapore Pte Ltd (the “Organisation”) notified the Personal Data Protection Commission (the “Commission”) that a server on the Organisation’s network which stored the personal data of its employees, among other information, had been the target of a ransomware attack. This attack resulted in the unauthorised encryption of the employee personal data hosted on that server and the Organisation being subjected to a ransom demand (the “Incident”). The Commission commenced an investigation in order to determine whether the Organisation had failed to comply with its obligations under the Personal Data Protection Act 2012¹ (the “PDPA”).

MATERIAL FACTS

2 The Organisation is a sushi chain restaurant. As part of its internal operations, it used an off-the-shelf payroll software application, “TimeSoft”, which was developed and licensed to it by Times Software Pte Ltd

1 Act 26 of 2012.

(“Times”). The TimeSoft application included a web portal and a database. The web portal was used by (a) employees to view their electronic payslips and (b) supervisors at the various restaurants to confirm the attendance of their employees during the designated hours. The database contained the personal data of the Organisation’s former and current employees (“Employee Data Files”). The TimeSoft application was hosted on a local server belonging to the Organisation (the “Server”). The Server also contained financial data files (*eg*, financial statements and details on the Organisation’s dealings with its vendors).

3 On 30 August 2018, the Organisation’s IT personnel discovered that the Server was unresponsive. Following internal investigations, the Organisation confirmed that the Server had been subjected to a ransomware attack, resulting in most of its hosted files (including the Employee Data Files) being encrypted with a “.bip” extension and their contents being inaccessible to the Organisation. A ransom payment was demanded from the Organisation in exchange for the decryption key. Based on its investigations, the Organisation suspected that the Server was infected by the “Dharma” variant of ransomware that had been installed on the Server through its Internet link.

4 The Incident resulted in the unauthorised modification of the Organisation’s data (including the Employee Data Files) as the encryption by the ransomware replaced the original plaintext with ciphertext (which was unreadable without the proper cipher to decrypt it). The following types of personal data belonging to approximately 360 current and former employees of the Organisation were affected by the unauthorised modification:

- (a) name;
- (b) NRIC number, if the employee was a Singaporean;
- (c) Foreign Identity Number (“FIN”) and application date, if the employee was a foreigner;
- (d) bank account information, *ie*, bank and branch information;
- (e) gender;
- (f) marital status;
- (g) date of hire;
- (h) date of birth; and
- (i) salary details.

5 The Incident also affected the following types of personal data for some of the Organisation's current or former employees (who had these types of data stored in the Server):

- (a) passport number;
- (b) address;
- (c) telephone number;
- (d) mobile phone number;
- (e) names of relatives;
- (f) emergency contact person's name and relationship with the employee; and
- (g) country of birth.

6 There was no evidence of the encrypted personal data files being subjected to exfiltration or unauthorised disclosure.

7 Upon discovery of the Incident, the Organisation immediately took the following steps to contain and mitigate the effects of the Incident:

- (a) isolated the Server from its larger IT network;
- (b) performed anti-virus scans on each computer in the Organisation's office and restaurants;
- (c) attempted, albeit unsuccessfully, to remove the ransomware and decrypt the infected data files using third-party security tools; and
- (d) to the best of its ability, notified its affected employees of the Incident. In this regard, all full-time employees and most part-time employees were notified by 7 September 2018. The Organisation was unable to notify its affected former employees due to their contact details being encrypted by the ransomware.

8 The Organisation subsequently also took the following steps to prevent the recurrence of the Incident:

- (a) replaced the Server with a new server that was isolated in a "de-militarised zone" within the Organisation's IT network;
- (b) introduced the following safeguards to protect the personal data in the new server:
 - (i) encrypting the TimeSoft application's database;
 - (ii) setting the server's firewall security policy to allow traffic only via Hyper Text Transfer Protocol Secure or through required service ports;

- (iii) enabling an intrusion prevention system on the firewall;
- (iv) installing TrendMicro OfficeScan XS anti-virus software on the new server, with the intent of subsequently upgrading this software to TrendMicro Deep Security after improvements to the Organisation's overall enterprise IT structure are completed;
- (v) enabling audit logging on the new server;
- (c) engaged an external vendor to provide security operation centre services, whereby the vendor would monitor the network and server logs and look out for any potential malicious activities on the new server; and
- (d) engaged an IT security vendor to assist with updating the Server's operating system, managing patches for the Server, and conducting regular IT vulnerability assessments.

FINDINGS AND BASIS FOR DETERMINATION

9 The main issue for determination is whether the Organisation breached s 24 of the PDPA. 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.

10 As a preliminary point, it is noted that, during the material time, the Organisation was responsible for the maintenance of the Server, while Times was in charge of providing technical support for the TimeSoft application, such as maintaining its web portal and database, as well as troubleshooting the application. Times provided its technical support on an *ad hoc* basis via remote access granted by the Organisation. During this process, the Organisation's IT personnel would supervise the activities of Times to ensure that there was no unauthorised access to, or collection of, the personal data hosted on the Server. Accordingly, Times did not have any control or possession of the personal data hosted on the Server. In any event, the Incident did not relate to the scope of Times' services rendered to the Organisation. As such, the Commissioner found that only the Organisation was in possession and control of the personal data, including the Employee Data Files, hosted on the Server during the material time.

11 To determine whether the Organisation was in breach of s 24, the relevant question is whether it had put in place reasonable security arrangements to safeguard the personal data hosted on the Server. The Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*² provide the following examples of factors that are taken into consideration in assessing the reasonableness of an organisation's security arrangements:

- (a) the nature of the personal data;
- (b) the form in which the personal data has been collected (eg, physical or electronic); and
- (c) the possible impact on the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

12 In assessing the security arrangements adopted by the Organisation, the Commissioner considered that the Employee Data Files included sensitive personal data in the form of NRIC numbers, FINs, passport numbers, bank account details and salary details. In this regard, it bears repeating what was stated in *Re Aviva Ltd*:³

All forms or categories of personal data are not equal; organisations need to take into account the sensitivity of the personal data that they handle. In this regard, the Commissioner repeats the explanation in *Re Aviva Ltd* [2017] (at [18]) on the *higher standards of protection that should be implemented for sensitive personal data*:

The Advisory Guidelines on Key Concepts in the Personal Data Protection Act states that an organisation should 'implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity'. *This means that a higher standard of protection is required for more sensitive personal data. More sensitive personal data, such as insurance, medical and financial data, should be accorded a commensurate level of protection.* In addition, the *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data* expressly states that documents that contain sensitive personal data should be 'processed and sent with particular care'.

[emphasis added]

2 Revised 27 July 2017, at para 17.2.

3 [2019] PDP Digest 145 at [17].

13 It should also be borne in mind that NRIC numbers are of special concern as they are “a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual”.⁴

14 The standard of security arrangements expected in relation to IT systems was elaborated upon in *Re The Cellar Door Pte Ltd*;⁵ “reasonable security arrangements” for IT systems must be sufficiently robust and comprehensive to guard against a possible intrusion or attack:⁶

Another important aspect of a ‘reasonable security arrangement’ for IT systems is that *it must be sufficiently robust and comprehensive to guard against a possible intrusion or attack*. For example, it is not enough for an IT system to have strong firewalls if there is a weak administrative password which an intruder can ‘guess’ to enter the system. The nature of such systems require there to be sufficient coverage and an adequate level of protection of the security measures that are put in place, since a single point of entry is all an intruder needs to gain access to the personal data held on a system. In other words, *an organisation needs to have an ‘all-round’ security of its system. This is not to say that the security measures or the coverage need to be ‘perfect’, but only requires that such arrangements be ‘reasonable’ in the circumstances*. [emphasis added]

15 In this case, the Organisation had failed to put in such “all-round” security of its system which is accessible via the Internet by all of its branches, and which contained sensitive personal data of its employees, *eg*, NRIC/FIN and passport numbers, and bank account details. The Commission’s investigations revealed the following significant gaps in the security measures implemented in relation to the Server during the Incident:

- (a) first, the Organisation initially did not have a firewall for the Server and, even after a firewall had been installed following its recent IT migration pursuant to its business re-organisation, it failed to configure the Server’s firewall to filter out unauthorised traffic and close unused ports;
- (b) second, the Organisation did not conduct periodic penetration tests to assess the overall security of its IT infrastructure and bolster the effectiveness of its defensive mechanisms and

4 *Re Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [19].

5 [2017] PDP Digest 160.

6 *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [29].

determine what measures (including patches) may be required to fix vulnerabilities; and

- (c) third, the Organisation failed to ensure that the Server and the TimeSoft application were regularly patched.

16 As regards the failure in [15(a)] above, although the Server was kept in a secure physical location with physical access only granted to authorised personnel, the same level of precaution had not been implemented for virtual or remote access. There was no firewall for a while, and even when installed, the Server's firewall was not configured to block any unused ports or unauthorised traffic at all material times. In other words, the Server's firewall was ineffective at filtering out any external threats.

17 In its response to the Commission's queries, the Organisation had explained that the lack of configuration for the firewall was because the Organisation had recently undergone a full IT migration and its IT team was waiting for the IT infrastructure to be refreshed before configuring the appropriate firewall settings. Pending this refresh, it had not configured any firewall setting as the Organisation did not have any server firewall before the IT migration and therefore no pre-existing configuration it could use for the firewall in the interim period. Thus, there was effectively no firewall in place during the relevant period.

18 The Commissioner reiterates what was said in *Re The Cellar Door* that "a firewall is *fundamental* to the security of the server to protect against an array of external cyber threats" and "leaving unused ports on a server open increases the risk of an external hacker exploiting the services running on these ports".⁷ In this case, the firewall was not configured to close *any* ports.

19 As regards the failures in [15(b)] and [15(c)] above, the Organisation admitted that it had not conducted any penetration tests on the Server within the last 12 months prior to the Incident. The Organisation was also unable to provide evidence that it had done any patching on the Server during the same period. This suggests that the Organisation did not have any processes in place to ensure regular security testing and patching of its IT systems.

20 The Commissioner emphasises that regular security testing and patching are important security measures. Patching is one of the common

⁷ *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [30(a)] and [30(b)].

tasks that all system owners are required to perform in order to keep their security measures current against external threats. Moreover, as stated in the Commission's *Guide to Securing Personal Data in Electronic Medium*:⁸

Vulnerabilities discovered [in software] are often published, hence cyber attackers are well aware of vulnerabilities available for exploiting.

It is therefore important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities.

21 Generally, organisations should, to the extent possible, test and apply updates and security patches as soon as they are available to the relevant components (*eg*, network devices, servers, database products, operating systems, applications, software libraries, programming frameworks and firmware) of the organisation's IT system. There should also be processes and people responsible to monitor new patches and updates that become available with respect to such components. In this regard, the arrangement with Times for maintenance and technical support of the TimeSoft application was inadequate.

22 The failures highlighted above contributed to a system that had a number of vulnerabilities and gaps that a hacker could easily exploit. In this case, the ransomware may have successfully exploited these gaps to reach the Employee Data Files and the other files on the Server. For a server that held sensitive personal data, the security measures implemented by the Organisation were inadequate. In fact, the standard of protection provided was not even sufficient for non-sensitive personal data.

23 For the reasons above, the Commissioner finds the Organisation in breach of s 24 of the PDPA.

REPRESENTATIONS BY THE ORGANISATION

24 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose. The Organisation raised the following factors for the Commissioner's consideration:

- (a) there was no evidence that the personal data had been subjected to exfiltration, unauthorised disclosure or modification;

8 Revised 20 January 2017, at paras 16.3 and 16.4.

- (b) the Organisation did not pay the ransom amount to positively discourage and disincentivise unauthorised and criminal behaviour by the ransomware attacker; and
- (c) the Incident occurred during the period where the Organisation's new management was in the midst of the IT migration and strengthening of the IT infrastructure.

25 The Commissioner has decided to maintain the financial penalty set out at [29] below for the following reasons:

- (a) As explained at [4] above, there had been unauthorised modification to personal data belonging to approximately 360 current and former employees of the Organisation. In determining the quantum of financial penalty, the Commissioner had already taken into consideration that there was no evidence of the encrypted Employee Data Files being subjected to exfiltration or unauthorised disclosure.
- (b) Notwithstanding that there was criminal activity on the part of the ransomware attacker, the finding of a s 24 breach relates to the Organisation's own failings to put in place reasonable security measures. As such, whether the ransom amount is paid is not a mitigating factor.
- (c) A transition to a new management team does not lower the standard expected of an organisation to protect personal data in its possession and/or control. Notwithstanding that the Organisation was in the midst of IT migration and strengthening of IT infrastructure, it was obliged to put in place reasonable security measures to protect the Employee Data Files at all times. These are therefore not mitigating factors. In any event, as stated at [15] above, the Commission's investigations revealed that the Organisation did not have adequate security measures in place for the Server even before the IT migration.

THE COMMISSIONER'S DIRECTIONS

26 Given 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 issue the Organisation such directions as he deems fit to ensure its compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding \$1m.

27 In determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account the following mitigating factors:

- (a) the Organisation voluntarily notified the Commission of the breach;
- (b) the Organisation fully co-operated with the Commission's investigations; and
- (c) the Organisation took prompt action to mitigate the effects of the breach.

28 The Commissioner also took into account, as an aggravating factor, that the failure to make reasonable security arrangements to protect the personal data led to a loss of control over the Employee Data Files, which contained sensitive personal data.

29 Taking into account the above mitigating and aggravating factors, the Commissioner hereby directs the Organisation to pay a financial penalty of \$16,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁹ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until it is paid in full.

30 The Commissioner has not set out any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

9 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Horizon Fast Ferry Pte Ltd

[2020] PDP Digest 357

Coram: Tan Kiat How, Commissioner

Case Number: DP-1710-B1202

Decision Citation: [2020] PDP Digest 357; [2019] SGPDPDC 27

Openness Obligation – Failure to appoint data protection officer
Openness Obligation – Lack of data protection policies and practices
Protection Obligation – Disclosure of personal data – Insufficient administrative security arrangements

25 July 2019

1 On 9 October 2017, the complainant (“Complainant”) informed the Personal Data Protection Commission (the “Commission”) that by entering her passport number in the booking form on the Organisation’s website, her name, gender, nationality, date of birth and passport expiry date were automatically populated in the corresponding fields on the form on the booking site without any requirement for further authentication (the “Incident”).

MATERIAL FACTS

2 The organisation (“Organisation”) is a Singapore-based ferry operator with ferry services running between Singapore and Batam.

3 As part of its service offerings, the Organisation operates a website that allows passengers to purchase ferry tickets directly from the Organisation online (“Booking Site”). At the material time, passengers who wanted to purchase ferry tickets through the Booking Site were required to provide the following personal data (the “Personal Data Set”) as set out in the form on the Booking Site (“Booking Form”):

- (a) the passenger’s full name;
- (b) gender;
- (c) nationality;

- (d) date of birth;
- (e) passport number; and
- (f) passport expiry date.

4 The same Personal Data Set was collected from passengers and entered into the Organisation's counter check-in system ("CCIS") when they checked in at the check-in counter. The CCIS is an internal system used by the Organisation's counter staff to manage the passenger check-in process and is only accessible by authorised counter staff.

5 As a matter of practice, all Personal Data Sets collected from the Booking Site and the CCIS were stored and retained on the Organisation's internal database (the "Database") even after the last travelling date of the passenger's itinerary to facilitate and speed up subsequent check-ins for passengers who have previously travelled with the Organisation ("Returning Passengers").¹

6 In this regard, one of the features of the CCIS was the auto-retrieval of the personal data of Returning Passengers. By entering a Returning Passenger's passport number, the CCIS would automatically retrieve the Personal Data Set associated with a Returning Passenger's passport number from the Database and populate the remaining fields in the Booking Form. Counter staff would no longer need to manually enter the Returning Passenger's personal data. The personal data retrieved from the Database was only meant to be accessible by authorised counter staff on the CCIS.

Booking Site revamp

7 In or around May 2017, the Organisation engaged an independent contractor (the "Contractor") on an informal basis to revamp the Booking Site, specifically to improve the user interface and user experience, such as when purchasing ferry tickets online. The parties did not enter into any written contract for the revamping of the Booking Site and all instructions and requirements for the revamp of the Booking Site were conveyed either verbally or through WhatsApp text messages. The Organisation did not inform or instruct the Contractor of its data protection obligations in relation to the personal data in the Database.

1 The Organisation also represented that the Personal Data Sets were retained on the Database for audit and accounting and internal reporting purposes.

8 Unbeknownst to the Organisation and contrary to its intention, the Contractor replicated the auto-retrieval and auto-population feature (which was only meant to be used in the internal CCIS) in the Booking Site as part of the website revamp. Consequently, whenever a user entered a passport number which matched a Returning Passenger's passport number in the Database, the system would automatically retrieve and populate the remaining fields in the Booking Form with the Personal Data Set associated with the Returning Passenger's passport number. As the Organisation failed to conduct proper user acceptance tests before launching the revamped Booking Site, the Organisation was not aware of this function until it was notified of the Incident.

9 At the time of the investigation, there were a total of 444,000 Personal Data Sets stored in the Database.² However, the Organisation represented that out of the 444,000 Personal Data Sets, there were only a total of 295,151 unique passengers whose Personal Data Sets were stored in the Database as a number of passengers had made bookings under different passport numbers (valid and expired).³

10 The Organisation took the following remedial actions shortly after it was notified of the Incident:

- (a) the Organisation commenced investigations and removed the auto-retrieval and auto-population feature from the Booking Site a little more than a week after the Organisation was first notified of the Incident;
- (b) the Organisation conducted checks to ensure that the auto-retrieval and auto-population feature was disabled from the Booking Site; and
- (c) the Organisation implemented administrative measures to protect the personal data in its possession, such as ensuring that documents containing booking data and passenger manifests were properly shredded at the end of the day, that monthly reports with passenger data were kept in a locked room and sent

2 Approximately three months after the date of the complaint, on 12 December 2017.

3 Other than the Personal Data Sets, some users also supplied their mobile phone numbers. There were 5,218 unique mobile numbers collected and stored in the Database as at 12 December 2017.

for mass disposal at the end of the financial year and the Organisation appointed a data protection officer to be responsible for ensuring the Organisation's compliance with the Personal Data Protection Act 2012 ("PDPA").⁴

FINDINGS AND BASIS FOR DETERMINATION

11 The two main issues for determination are:

- (a) whether the Organisation complied with its obligations under ss 11(3) and 12(a) of the PDPA; and
- (b) whether the Organisation breached s 24 of the PDPA.

12 The Personal Data Sets stored in the Database are "personal data" as defined in s 2(1) of the PDPA. In particular, given that the unauthorised disclosure of the Personal Data Set as a whole could have led to an increased risk of such personal data being used for illegal activities such as identity theft or fraud, they are personal data of a more sensitive nature.⁵

Whether the Organisation complied with its obligations under sections 11(3) and 12(a) of the Personal Data Protection Act 2012

13 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring compliance with the PDPA. In a similar vein, 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, the "Openness Obligation").

14 As mentioned above, all passengers who purchased ferry tickets from the Organisation were required to provide the personal data in the Personal Data Set to the Organisation either at the time of booking through the Booking Site or at the Organisation's check-in counter.

15 However, even though the Organisation routinely collected and processed large volumes of personal data in the course of its business, the Organisation demonstrated a blatant disregard for its data protection obligations.

4 Act 26 of 2012.

5 See *Re Singapore Management University Alumni Association* [2019] PDP Digest 170 at [20].

16 By its own admission, at the time of the Incident, the Organisation did not designate any individual to be responsible for ensuring that the Organisation complies with the PDPA, *ie*, a data protection officer (“DPO”). The Organisation’s current DPO was only appointed after 6 November 2017, when the Organisation was first informed of the Incident.

17 Similarly, the Organisation’s privacy policy was only implemented and uploaded on its Booking Site after it was informed of the Incident. While the Organisation represented that it had an internal guideline titled “Workplace policies: confidentiality” in place at the time of the Incident, apart from a reference to its commitment to “[e]stablish data protection practices (e.g. secure locks, data encryption, frequent backups, access authorization)”, the internal guidelines do not set out any actual practices or processes to protect the personal data in the Organisation’s possession.

18 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. This was highlighted in *Re M Stars Movers & Logistics Specialist Pte Ltd*⁶ (“*M Stars Movers*”):

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).

6 [2018] PDP Digest 259 at [27] and [28].

19 Likewise, 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 regardless of the size of the organisation.⁷

20 As highlighted in *M Stars Movers*, 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.

21 In the circumstances, it is clear that the Organisation failed to meet its obligations under ss 11(3) and 12(a) of the PDPA. Had the Organisation met its Openness Obligation under the PDPA, the Organisation would have had a clearer understanding of its data protection obligations under the PDPA and appropriate measures may have been put in place earlier which could have prevented the Incident from occurring.

Whether the Organisation breached the Protection Obligation under the Personal Data Protection Act 2012

22 As a preliminary point, although the Contractor appears to have been responsible for carrying out the Booking Site revamp, seeing as the parties did not enter into any written agreement and there was no evidence to suggest that the Contractor stored, held or managed the personal data in the Database on behalf of the Organisation, the Contractor is not a data

7 *Re M Star Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [37].

8 *Re M Star Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [34].

intermediary of the Organisation. The Organisation is solely responsible for complying with all the data protection obligations under the PDPA, including the obligation to make reasonable security arrangements to protect the personal data in its possession or under its control under s 24 of the PDPA.

23 At the time of the Incident, the Database was shared by the Booking Site and the CCIS. However, the Organisation conceded that it omitted to inform the Contractor of its data protection obligations and did not instruct the Contractor to put in place proper safeguards to protect the personal data in the Organisation's possession or control.

24 In this regard, one of the key considerations for organisations as highlighted in the *Guide on Building Websites for SMEs*⁹ is the importance of emphasising the need for personal data protection to their IT vendors:

Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:

- Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.
- Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet.
- Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.
- When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.

9 Personal Data Protection Commission, *Guide on Building Websites for SMEs* at para 4.2.1.

25 Even more concerning was the fact that the Organisation did not put in place reasonable arrangements to discover risks to its personal data when changes were made to the Booking Site that was linked to the Database which held the personal data of close to 300,000 individuals. The Organisation did not conduct any proper user acceptance testing prior to the launch of the revamped Booking Site. The only test that the Organisation carried out was to key in a simulated passport number to test the new user interface. However, as the simulated passport number did not match any record in the Database, the Organisation failed to detect the auto-retrieval and population feature in the revamped Booking Site.

26 Websites connected to the Internet are subject to a multitude of cyber threats that may compromise the website and expose any personal data it collects. Organisations should therefore ensure that the protection of the personal data and the security of the website is a key design consideration at each stage of the website's life cycle – be it during the requirements gathering, design and development stage or when conducting user acceptance testing or deployment and operations and support.¹⁰

27 As a result of the Organisation's failure to conduct proper user acceptance tests, the gap in the revamped Booking Site which allowed for the unauthorised access to personal data stored in the Database went undetected. This was not rectified for approximately one month, thereby causing the personal data of close to 300,000 of the Organisation's passengers to be exposed to the risks of unauthorised disclosure.

28 As a matter of good practice, organisations should consider whether there is a need to conduct a data protection impact assessment whenever a new system or process is being introduced, developed or implemented that involves the handling of personal data or an existing system or process is being reviewed or substantially redesigned.¹¹

10 See Personal Data Protection Commission, *Guide on Building Websites for SMEs* at paras 3.2–3.3.

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

29 In this regard, the *Guide to Data Protection Impact Assessments*¹² states that:

A [Data Protection Impact Assessment] involves identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes. In doing so, an organisation would be better positioned to assess if their handling of personal data complies with the PDPA or data protection best practices, and implement appropriate technical or organisational measures to safeguard against data protection risks to individuals.

30 In adopting this view, the Commissioner agrees with the observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia on the proper use of risk assessment tools for all new projects involving personal information:¹³

Privacy risks evolve over time. Conducting risk assessments, at least on an annual basis, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.

We have seen instances of organizations offering new services that collect, use or disclose personal information that have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a privacy problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any privacy impacts beforehand is vital.

12 Personal Data Protection Commission, *Guide to Data Protection Impact Assessments* (1 November 2017) at para 1.2.

13 Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, "Getting Accountability Right with a Privacy Management Program" (April 2012) <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-compliance-and-training-tools/gl_acc_201204/> (accessed 27 March 2020).

As a result, such assessments should be required throughout the organization for all new projects involving personal information and on any new collection, use or disclosure of personal information. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.

[emphasis added]

31 In view of the above and the Organisation’s failure to put in place adequate security arrangements to protect the personal data in the Database, the Commissioner finds that the Organisation was in breach of the Protection Obligation under s 24 of the PDPA.

32 Finally, although the Organisation did not intend to offer the auto-retrieval and auto-population function on its Booking Site, organisations that do offer such functions should take note of the following comments made by the UK Information Commissioner’s Office (“ICO”) in the *Personal Information Online Code of Practice* on the use of auto-completion facilities for forms and passwords:

If your site offers auto-completion facilities for forms and passwords, it is good practice to notify users if this could leave them vulnerable, for example if their mobile device or laptop is stolen. However, ultimately users have a role to play in protecting themselves online, for example by adjusting the auto-complete settings on their browser or on a website they visit. *Autocompletion can present a particular risk where an individual’s payment card details have been retained for ‘auto-fill’ purposes. This may mean not offering auto-completion in certain contexts – e.g. on password fields for authorising payments.* [emphasis added]

DIRECTIONS

33 Having found that the Organisation is in breach of ss 11(3), 12(a) and 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding \$1m.

34 In deciding whether to direct an organisation to pay a financial penalty, one of the Commissioner’s key objectives is to promote compliance with the PDPA. As such, while the Commissioner will seek to ensure that the financial penalty imposed is reasonable and proportionate on the facts, the financial penalty should also be sufficiently meaningful to act both as

a sanction and as a deterrent to prevent similar contraventions of the PDPA.

35 In this regard, as highlighted in the *Advisory Guidelines on Enforcement of the Data Protection Provisions*,¹⁴ the Commissioner will take into account factors such as the seriousness and impact of the organisation's breach and will consider if the organisation had acted deliberately, wilfully or if the organisation had known or ought to have known of the risk of a serious contravention and failed to take reasonable steps to prevent it.

36 In adopting this view, the Commissioner agrees with the ICO's *Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55C(1) of the Data Protection Act 1998*¹⁵ ("ICO Guidance on Monetary Penalties"):

The Commissioner's aim in imposing a monetary penalty

34. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA or with PECR.
35. The penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others.
36. This applies both in relation to the specific type of contravention and other contraventions more generally. Here, the Commissioner will have regard to the general approach set out in paragraphs 42 to 46 below.
37. The Commissioner will seek to ensure that the imposition of a monetary penalty is appropriate and the amount of that penalty is reasonable and proportionate, given the particular facts of the case and the underlying objective in imposing the penalty.

37 With the foregoing principles in mind, the Commissioner took into account the following aggravating and mitigating factors in assessing the breach and determining the directions to be imposed:

Aggravating factors

- (a) The Organisation routinely collects and processes the personal data of a large number of individuals in the course of its business

14 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* at para 24.1.

15 At paras 34–37.

but did not have adequate data protection policies or practices in place.

- (b) The Personal Data Sets collected and stored in the Database, such as the individual's nationality, passport number and passport expiry date, are of a sensitive nature particularly when disclosed as a whole. In this regard, attention is drawn to the decision in *Re Singapore Management University Alumni Association*¹⁶ ("SMU AA") where it was stated that "the use of an NRIC number generation tool would make it relatively easy for a motivated hacker to systematically query the webpage and, if successful, he would have been able to definitively link the NRIC number to the full name, address and other personal data of the member, potentially resulting in significant harm to the individual, such as through identity theft or an unauthorised person impersonating the affected member".
- (c) The Organisation demonstrated a blatant lack of regard for its data protection obligations prior to the Incident. Despite the fact that the PDPA came into full force on 2 July 2014 and advisory guidelines and/or guides which are relevant to the contravention were available, the Organisation only appointed a DPO more than three years after the PDPA came into full force and appears to have ignored or not given these guidelines and/or guides the appropriate weight.
- (d) As a result of the Organisation's lack of regard for its data protection obligations, the personal data of at least 295,151 of the Organisation's passengers were exposed to the risks of unauthorised disclosure.

Mitigating factors

- (e) the Organisation had co-operated fully in the investigation and was forthcoming and transparent in admitting its mistakes in contributing to the unauthorised disclosure;
- (f) remedial actions were taken and the Organisation took increased efforts to heighten employees' awareness of the Organisation's data protection obligations under the PDPA;

16 [2019] PDP Digest 170 at [20].

- (g) there was no evidence to suggest any actual unauthorised access and/or exfiltration of data leading to loss or damage; and
- (h) there was limited disclosure to possibly one individual who would have had to enter a Returning Passenger's passport number that matched the passport number in the Database.

38 The Organisation submitted representations, after being informed of the proposed decision in this case, requesting a warning in lieu of a financial penalty or otherwise to reduce the quantum of the financial penalty imposed. In support of this, the Organisation made the following representations:

- (a) The Organisation asserted that the revamped Booking Site was only operational in or around October 2017, and the auto-retrieval and auto-population feature was only accessible to users (other than the authorised counter staff) from October 2017 to 14 November 2017. Thus, the Personal Data Sets were only at risk of unauthorised disclosure for this period of time.
- (b) The Organisation did not deliberately or wilfully breach the PDPA, and upon notification of the Incident, the Organisation took remedial actions¹⁷ and was co-operative during the investigations.
- (c) The risk of unauthorised disclosure is low as an individual would need to possess the exact passport number to trigger the auto-complete feature which would disclose the corresponding Personal Data Set.

39 With respect to the issue raised in [38(a)] above, the Commissioner accepted the clarifications as to the period of time for which the Personal Data Sets were at risk of unauthorised disclosure, and the quantum of the financial penalty has been adjusted accordingly.

40 With regard to [38(b)] above, the remedial actions taken by the Organisation and the fact that the Organisation was co-operative during the investigations have already been taken into account as mitigating factors at [37(e)] and [37(f)] above in determining the appropriate quantum of the financial penalty. Also, the deliberateness or wilfulness of the Organisation in breaching the PDPA is not a relevant consideration in this case where it

17 Including those set out at [10] above.

was found that the Organisation failed to put in place the necessary security arrangements to protect the Personal Data Set.

41 With regard to [38(c)] above, these are matters that had already been taken into consideration in assessing the financial penalty and as set out at [37(g)] and [37(h)] above.

42 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of \$54,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court¹⁸ in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

18 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Avant Logistic Service Pte Ltd

[2020] PDP Digest 371

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1802-B1709

Decision Citation: [2020] PDP Digest 371; [2019] SGPDPDC 28

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

30 July 2019

BACKGROUND

1 On 25 November 2017, a customer of Ezbuy Holdings Ltd (“Ezbuy”) made a complaint to the Personal Data Protection Commission (the “Commission”) alleging that her personal data had been disclosed to another customer of Ezbuy without her consent by an employee of Avant Logistic Service Pte Ltd (the “Organisation”). The facts of this case are as follows.

2 Ezbuy provides an online e-commerce platform that allows its customers to shop for items from various online retailers and platforms around the world. It engaged the Organisation to provide delivery services in Singapore. The Organisation is an affiliate of Ezbuy and its delivery personnel are required to adhere to Ezbuy’s Privacy Policy and the terms and conditions in Ezbuy’s Employee Handbook and Ezbuy’s Delivery and Collection Standard Operation Procedure (“SOP”).

3 When a customer ordered an item through Ezbuy’s platform, they would be offered two modes of delivery: (a) delivery to a designated collection point (referred to by Ezbuy as “self-collection”) or (b) delivery to the customer’s address. If the customer opted for self-collection, the customer would proceed to the designated collection point at a specified time. The delivery personnel there would verify their identity using their

Ezbuy user ID or their mobile number registered with Ezbuy and then hand over the package with their item.

4 On 9 November 2017, the complainant scheduled to self-collect a package that she ordered from Ezbuy at a collection point in Bishan at around 6.30pm. One of the Organisation’s employees (referred to in this decision as “OA”) was assigned to distribute packages there that evening. When the complainant met OA at the collection point, he gave the complainant two packages (the “Packages”) after verifying her identity. The complainant noticed that the Packages were not hers because they bore the user ID and mobile number of another person (referred to in this decision as “CA”). According to the complainant, she informed OA of this but was told to take the Packages as they were tagged to her mobile number in the Ezbuy system. The complainant also alleged that OA asked her to inform Ezbuy’s customer service that the wrong packages had been sent to her. The complainant then left the collection point with the Packages.

5 CA arrived to collect the Packages shortly after the complainant left. OA informed her that someone else had already collected the Packages and told her that he would try to locate them and arrange for their subsequent delivery. At this time, OA did not realise that it was the complainant who had collected the Packages.

6 Later that night, OA sent CA screenshots of two delivery lists containing Ezbuy user IDs and mobile telephone numbers of some Ezbuy customers (the “Disclosed Data”). The first list that was sent contained the Ezbuy user IDs and mobile telephone numbers of eight Ezbuy customers who had been scheduled to collect their packages at Bukit Panjang. (This was apparently sent by mistake.) The second list contained the user IDs of four Ezbuy customers, including that of the complainant, who had been scheduled to collect their packages at Bishan. The telephone numbers in the second list were redacted by OA. However, OA also sent the complainant’s mobile telephone number to CA. OA explained to CA that he suspected that the complainant had collected the Packages because his records showed that the complainant had not collected her own packages.

7 CA eventually managed to find the complainant’s Facebook and Instagram pages using the complainant’s Ezbuy user ID as the complainant had used the same name (which was not her real name) for her Facebook, Instagram and Ezbuy user IDs. CA then sent a series of messages to the

complainant via Facebook Messenger in order to recover the Packages. The complainant subsequently returned the Packages to Ezbuy.

Remedial actions by Ezbuy and the Organisation

8 After being informed of the incident by the Commission, Ezbuy and the Organisation jointly undertook the following measures to prevent the unauthorised disclosure of customers' personal data in the future:

- (a) all delivery personnel are required to request for *both* a customer's user ID and mobile telephone number for verification during the self-collection process;
- (b) Ezbuy's Delivery and Collection SOP was updated to comply with the provisions of the Personal Data Protection Act 2012¹ ("PDPA") and to highlight the importance of the PDPA. In particular, a clause was added by Ezbuy stating that no customer information can be disclosed to any party under all circumstances, and that any unauthorised disclosure will lead to disciplinary action as listed in Ezbuy's Employee Handbook;
- (c) a briefing was conducted to all delivery personnel to reinforce the instruction and policy that no customer's personal data should be provided to any third party under all circumstances, and this briefing is repeated to all delivery personnel every morning; and
- (d) Ezbuy revised its Employee Handbook to include detailed enforcement and disciplinary actions to be taken for breach of confidentiality and employee misconduct, including any leak or sale of customer data.

FINDINGS AND BASIS FOR DETERMINATION

Was the Disclosed Data personal data?

9 As a preliminary issue, I find that most of the Disclosed Data was personal data within the meaning of the PDPA. The term "personal data" is defined in s 2(1) of the PDPA as follows:

1 Act 26 of 2012.

‘personal data’ means data, whether true or not, about an individual who can be identified —

- (a) from that data [“Direct Identification”]; or
- (b) from that data and other information to which the organisation has or is likely to have access [“Indirect Identification”] ...

10 The mobile telephone numbers disclosed by OA constitute personal data since they enable Direct Identification of the respective individuals. As explained in the Commission’s *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*,² an individual’s personal mobile telephone number is a “unique identifier” and capable, on its own, of identifying the individual.

11 On the other hand, since Ezbuy user IDs do not enable Direct Identification, whether they qualify as “personal data” depends on whether they enable Indirect Identification. In this case, CA was able to find the complainant’s Facebook and Instagram pages and identify her using the complainant’s Ezbuy user ID. The complainant’s Ezbuy user ID therefore constitutes personal data under the PDPA, even though the user ID did not contain the complainant’s real name, as it enabled Indirect Identification of the complainant.

12 Although organisations cannot be expected to know in advance if the user IDs of their customers enable Indirect Identification, they should not assume that user IDs *per se* do not constitute personal data as such an assumption may not, in fact, be true (as seen from this case). Organisations should therefore exercise prudence in handling user IDs. As there is no evidence that the other Ezbuy user IDs in the Disclosed Data allowed for Indirect Identification, I grant the Organisation the benefit of the doubt and accept that they do not constitute personal data. Nevertheless, it remains that the personal data of nine individuals (corresponding to the nine mobile telephone numbers disclosed) was disclosed without their consent or the authorisation of the Organisation.

Whether the Organisation had made reasonable security arrangements

13 Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable

2 At paras 5.9–5.10.

security arrangements to prevent unauthorised use, disclosure and similar risks. Although the Organisation's delivery personnel were required to comply with Ezbuy's Privacy Policy and Employee Handbook, this was, at the time of the incident, inadequate as it did not inform employees of exactly what they were required to do in order to protect customers' personal data:

- (a) Ezbuy's Privacy Policy only stated its commitment to ensuring security of customer information and that "suitable physical, electronic and managerial procedures" had been put in place to safeguard customer information; and
- (b) Ezbuy's Employee Handbook only included a provision highlighting that customer information (among others) was confidential.

14 At the time of the incident, the Organisation had not made any effort to impress upon its delivery personnel the need to protect personal data in their possession. The Organisation did not have measures in place, such as policies or standard operating procedures, to prohibit the unauthorised use or disclosure of personal data by its delivery personnel. The Organisation also had not provided any instruction or training to its delivery personnel on the proper handling of personal data and on compliance with the PDPA.

15 In the course of the Commission's investigation, the Organisation sought to rely on a clause in OA's employment contract which prohibited him from disclosing confidential information, including customer information, without the Organisation's prior consent (the "Confidentiality Clause"). While such clauses are relevant to an organisation's security arrangements to protect personal data, they are insufficient on their own because they typically do not elaborate on what constitutes personal data, nor how employees should handle and protect it. Organisations are expected to provide their staff with *specific, practical instruction* on how to handle personal data and comply with the PDPA.³ This is particularly important for the Organisation's delivery personnel who frequently handle personal data and are on the frontline of the Organisation's customer-facing operations where the potential for improper use and disclosure of personal data cannot be ignored.

3 *Re Hazel Florist & Gifts Pte Ltd* [2018] PDP Digest 199 at [18].

16 In the circumstances, I find that the Organisation had not made reasonable security arrangements to protect the personal data comprised in the Disclosed Data. The Organisation is accordingly in breach of s 24 of the PDPA.

17 One additional point I wish to address is that when OA was asked about the incident, he claimed that he had given the complainant the Packages as the complainant had provided him with CA's Ezbuy user ID and mobile telephone number for verification. As there is no evidence that the complainant and CA were known to each other, I do not find OA's recollection of the events to be credible or acceptable. In any case, this does not detract from the above conclusion that the Organisation had failed to make reasonable security arrangements as required under s 24 of the PDPA.

OUTCOME

18 Taking the totality of the circumstances into account, I have decided not to impose a financial penalty in this case. In particular, I note that:

- (a) the breach was a one-off incident, with few affected individuals and relatively little personal data disclosed (comprising the nine mobile telephone numbers and user IDs);
- (b) the Organisation took prompt remedial actions to prevent a recurrence of such an incident; and
- (c) the Organisation was co-operative during investigations.

19 Instead, I have decided to issue the following directions to the Organisation to ensure its compliance with the PDPA:

- (a) to put in place the appropriate written policies and process safeguards which are necessary for it to protect personal data in its possession or under its control within 30 days from date of this direction;
- (b) to arrange for personal data protection training for its staff within 60 days from date of this direction; and
- (c) to inform the Commission in writing of the completion of each of the above within one week of completion.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Friends Provident International Limited

[2020] PDP Digest 377

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1805-B2112

Decision Citation: [2020] PDP Digest 377; [2019] SGPDPDC 29

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

30 July 2019

FACTS OF THIS CASE

1 Friends Provident International Limited is a company established in the Isle of Man which provides life assurance services in Singapore through a registered branch office (the “Organisation”). In the course of providing these services, it operates and maintains an online portal (the “Portal”) through which its policyholders can request for changes to their particulars, for example, contact details. On 10 May 2018, the Organisation notified the Personal Data Protection Commission (the “Commission”) of a data breach incident involving the disclosure of certain personal data of policyholders obtained from the Portal. The circumstances leading to the incident were as follows.

2 The Organisation’s policyholders and certain other authorised personnel could access the Portal via a “Secured Mailbox” webpage on the Organisation’s website (the “Secured Mailbox Webpage”). Policyholders could, as noted above, submit certain requests via the Portal and the Organisation’s authorised personnel accessed the Portal in order to process these requests. For this purpose, the Organisation’s authorised personnel could generate reports containing the data of policyholders who had made a request (“Reports”). These Reports were stored in the Portal and could be obtained thereafter by the Organisation’s authorised personnel.

3 The ability to generate and obtain Reports from the Portal was intended to be restricted to the Organisation's authorised personnel. To achieve this, when a user logged in to the Secured Mailbox Webpage, the system would determine whether the user was one of the Organisation's authorised personnel or a policyholder. If the user was one of the authorised personnel, a "Report" tab would be displayed in the Secured Mailbox Webpage which enabled the authorised personnel to generate and obtain Reports. The "Report" tab was hidden from the view of policyholders when they accessed the Secured Mailbox Webpage. Apart from hiding the "Report" tab, no additional or separate authorisation was necessary in order to generate and obtain Reports from the Portal and there was no subsequent verification (after the user logged in) as to whether the user was, in fact, authorised to generate and obtain the Reports via the "Report" tab.

4 As a result of a faulty JavaScript within the Secured Mailbox Webpage, the "Report" tab was visible to policyholders when they re-sized their desktop Internet browser to a smaller size or if they accessed the Secured Mailbox Webpage via a mobile device. As no verification or separate authorisation was required to access the "Report" tab and generate and obtain Reports, such policyholders were able to generate and obtain Reports from the Portal once the "Report" tab was visible (collectively referred to as the "Vulnerability").

5 The exploitability of the Vulnerability, which had likely existed since 30 September 2017 when the Secured Mailbox Webpage was introduced, was fortuitously resolved on 6 February 2018 when the Secured Mailbox Webpage was enhanced and backend verification was included. Unfortunately, on 12 December 2017, one of the Organisation's policyholders discovered that he could generate and obtain Reports from the Portal that contained the names, policy numbers and regions of residence of other policyholders. He subsequently reported this to the Monetary Authority of Singapore which, in turn, notified the Organisation of the incident (the "Reported Breach"). The Organisation had been unaware of the Vulnerability until it was notified of the Reported Breach.

6 The Organisation subsequently determined that before the Vulnerability was fixed, 42 Reports had been produced and downloaded by 21 policyholders or their advisers. The total number of individuals affected by this was estimated to be 240, 11 of whom had their policy numbers

disclosed. After the Reported Breach, the Organisation undertook the following as part of its remedial actions:

- (a) reviewed the Portal to ensure that the Reports were no longer accessible by unauthorised personnel;
- (b) conducted an initial risk assessment and commenced an immediate investigation into the Reported Breach;
- (c) imposed a requirement that regression testing must be conducted for mobile devices and different screen resolutions;
- (d) ensured that back-end access validation was in place on top of front-end validation;
- (e) ensured that all employees received training on data protection upon commencement of employment, which would be refreshed annually; and
- (f) contacted the policyholder who had generated and downloaded Reports on 12 December 2017 to ensure that he no longer held the Reports that he downloaded.

FINDINGS AND BASIS FOR DETERMINATION

7 Section 24 of the Personal Data Protection Act 2012¹ (the “PDPA”) requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, disclosure and similar risks. I find that the Organisation had not done so, and is in breach of s 24, for two main reasons: first, the manner in which the Organisation restricted access to the Reports was insufficient to prevent unauthorised access to the Reports and the personal data they contained and, secondly, the testing of the Secured Mailbox Webpage was inadequate.

8 On the first point, what is most striking in this case is the lack of an authorisation mechanism for access to the ability to generate and obtain Reports. Once a user gained access to the Secured Mailbox Webpage and could view the “Report” tab (in the circumstances noted above), no further authorisation or verification was required to generate and obtain Reports from the Portal via the “Report” tab. The only means the Organisation employed to limit access to the Reports was to hide the “Report” tab from

1 Act 26 of 2012.

the view of unauthorised persons. This was insufficient as there could be various ways in which the hidden tab could be revealed, even without the faulty JavaScript, such as by manipulating the scripts or widgets running on the Secured Mailbox Webpage.

9 On the second point, given that the Secured Mailbox Webpage was intended for use across a variety of devices and screens, testing should have been conducted across multiple browsers and devices. While organisations are not expected to test across all possible browsers and devices, testing should have been done on representative devices (in the present case, with different screen or browser sizes) based on the design and intended functionality of the Secured Mailbox Webpage. The Organisation's failure to do so meant that its testing was ultimately inadequate to address the risk of unauthorised access to the personal data in the Reports. In fact, simply accessing the Secured Mailbox Webpage on a mobile device as part of its tests would have revealed the Vulnerability to the Organisation. Additionally, organisations and developers should note that the testing of other browser conditions such as script blocking, while not mandatory, is highly recommended. In the Organisation's case, script blocking would also have caused the "Report" tab to become visible.

OUTCOME

10 Taking the totality of the circumstances into account, I have decided to issue a warning to the Organisation for its contravention of s 24 of the PDPA. In reaching this conclusion, I note that:

- (a) the potential for misuse of the personal data disclosed was relatively low because the data was not of a nature where identity theft could be committed; and
- (b) the Organisation had promptly notified the Commission and implemented remedial actions upon learning of the Reported Breach.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Executive Link Services Pte Ltd

[2020] PDP Digest 381

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1806-B2237

Decision Citation: [2020] PDP Digest 381; [2019] SGPDPDC 30

Accountability Obligation – Lack of data protection policies and practices – Failure to appoint data protection officer

Protection Obligation – No finding of insufficient security arrangements

20 August 2019

BACKGROUND

1 On 11 June 2018, Executive Link Services Pte Ltd (the “Organisation”) reported a data breach to the Personal Data Protection Commission (the “Commission”) concerning the unintended disclosure of personal data of individuals that were stored on the Organisation’s server (“Incident”). The Commission investigated the Incident and determined that the Organisation had breached its obligations under the Personal Data Protection Act 2012¹ (“PDPA”).

MATERIAL FACTS

2 The Organisation is an employment agency. Sometime before 8 June 2018, one of the Organisation’s clients engaged a cybersecurity company to scan the Internet for information relating to the client. During this scan, the cybersecurity company was able to gain access to and retrieve copies of draft contracts of job candidates from the Organisation’s server. The Organisation was alerted on 8 June 2018. In total, resumes of 367 individuals (the “Affected Individuals”) and around 150 draft contracts

1 Act 26 of 2012.

relating to some of those individuals, together with the personal data therein (the “Compromised Personal Data”), were exposed to unauthorised disclosure in this manner.

3 The Compromised Personal Data included the following:

- (a) the individual’s name, address, contact number, e-mail address(es), education level, salary expectation and employment history (in relation to the resumes); and
- (b) the individual’s name, address and salary information (in relation to the draft contracts).

Events leading to the Incident

4 The Organisation had implemented remote access for staff to access internal files stored on its data storage server. This required the use of a virtual private network (“VPN”) service. The server was supplied by Blumm Technology Pte Ltd (“Blumm”) and installed and set up by the Organisation’s IT vendor, SShang Systems (“SShang”). SShang provided IT support services to the Organisation, *eg*, upgrading and configuration of hardware, and general IT troubleshooting. When staff had difficulties with VPN access, the Organisation approached SShang for assistance. SShang was, in turn, advised by Blumm to adopt a workaround, by opening and enabling file access through the server’s file transport protocol (“FTP”) port (the “VPN Workaround”). Blumm also advised SShang to password-protect the folders within the server after the FTP port was opened.

5 When SShang implemented the VPN Workaround, it did not advise the Organisation about password-protecting the folders on the server because it assessed that there was little or no risk of unauthorised access to the folders since remote access was limited to staff. Although the Organisation had only intended to test the VPN Workaround for a few days, it was during this period that its client discovered the Compromised Personal Data on its server.

6 In the course of the Commission’s investigation, the Organisation also admitted that it had not appointed a data protection officer (“DPO”) and that it did not have any policies, internal guidelines or procedures on the collection, use and disclosure of personal data and other matters required under the PDPA.

FINDINGS AND BASIS FOR DETERMINATION

Issues for determination

7 Based on the facts of the case, the issues to be determined are as follows:

- (a) whether the Organisation had complied with its obligation to protect personal data under s 24 of the PDPA; and
- (b) whether the Organisation had complied with the obligations to appoint a DPO and develop and implement data protection policies and practices under ss 11(3) and 12, respectively, of the PDPA.

Whether the Organisation complied with its obligation under section 24 of the Personal Data Protection Act 2012

8 At all material times, the Compromised Personal Data was in the Organisation's sole possession and control. SShang was engaged to provide IT support services but was not engaged to process personal data. Blumm supplied the server and had assisted to open the server's FTP port to enable the VPN Workaround, but it was not engaged to process personal data. Hence, both SShang and Blumm were not data intermediaries, and the responsibility to protect the Compromised Personal Data fell squarely and solely on the Organisation.

9 The question is whether the Organisation had failed to take reasonable steps to protect the Compromised Personal Data. It should be noted from the outset that this was not a case involving a server hosting a website that was meant to be accessible on the World Wide Web. It was an internal server that was meant to be accessed by staff remotely through the Internet. There are subtle but significant differences between the two. A website on the World Wide Web is by its nature intended to be more easily linked from other websites, and to be discovered by search engines and directories. Remote access to a server via the Internet requires the member of staff to use VPN software or know the precise Internet Protocol ("IP") address. It is not usually crawled by online search engines. But that is not to say that it cannot be discovered. It can be, by using the right tool to scan a known set of IP address range, as was done in this case by the

cybersecurity company. The footprint is smaller and the risk is lower, but that does not in any way mean that the risk does not exist.

10 The Organisation did not have requisite IT knowledge and depended on its outsourced IT support services provider. Its duties as owner of the server and controller of the Compromised Personal Data include making its requirements known to SShang and asking the right questions from the perspective of a business owner. It can rely on SShang's technical know-how. In this case, the Organisation was aware of the risks and had implemented VPN access for its staff. When there were difficulties with the VPN access and SShang was called upon to troubleshoot, it was a natural and reasonable expectation that any workaround recommended would not materially compromise its requirement for security. It is not unreasonable for the Organisation to have expected that any such material deviation – particularly when the security level is lowered – would be drawn to its attention.

11 Of course, the Organisation could have asked about the security of the VPN Workaround. But is it reasonable to expect this level of pedantry? I am mindful that when troubleshooting IT issues, there is a degree of urgency and need for speed to implement workarounds, identify root causes and implement permanent solutions. In these circumstances, the operating assumption should be that existing business rules continue to be relevant. However, I am of the view that since the VPN Workaround touched on secured remote access, the Organisation could have sought clarification of the impact of the VPN Workaround on its requirements for security.

12 In this case, SShang had been advised by Blumm to enable password protection. SShang had assessed that there was no need to do so as remote access was limited to staff and there was little or no risk of unauthorised access to the folders. We do not know what SShang would have informed the Organisation had the Organisation sought clarification. However, even if SShang shared its assessment and maintained its advice that it was not necessary to enable password protection, the Organisation would not have known better and would have relied on the advice. In the light of these circumstances, I am giving the Organisation the benefit of the doubt and will not make a finding of breach of its protection obligation under s 24 of the PDPA.

Whether the Organisation complied with its obligations under sections 11(3) and 12 of the Personal Data Protection Act 2012

13 The remaining two issues are straightforward. Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as the DPO. Further, s 12 of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to communicate information about such policies and practices to its employees (among other obligations). The importance of these requirements has been emphasised multiple times in previous decisions.²

14 In view of the Organisation's admissions that it had not appointed a DPO and had not developed and implemented any policies, internal guidelines or procedures on the collection, use and disclosure of personal data, I find the Organisation in breach of ss 11(3) and 12 of the PDPA.

REMEDIAL ACTIONS BY THE ORGANISATION

15 After being informed of the Incident by its client, the Organisation closed the FTP port on the same day. The Organisation also took the following additional steps:

- (a) shut down the server permanently and replaced it with a new server;
- (b) installed a firewall for the new server and implemented access to the new server via VPN, which requires the use of passwords (thereby limiting access to the data stored on the server);
- (c) implemented password policies for its employees for the use of the VPN;
- (d) engaged a cybersecurity firm to conduct a network vulnerability assessment on its new server, which found no vulnerabilities;
- (e) appointed a DPO;

2 See *Re Aviva Ltd* [2018] PDP Digest 245 at [32]; *Re M Stars Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [31]–[37]; *Re Singapore Taekwondo Federation* [2019] PDP Digest 247 at [39]–[42]; and *Re AgcDesign Pte Ltd* [2020] PDP Digest 322 at [4]–[5].

- (f) drafted and implemented policies on the handling of personal data; and
- (g) provided data protection training for its employees.

THE DEPUTY COMMISSIONER'S DIRECTIONS

16 In assessing the breach, I took into account the following mitigating factors:

- (a) The Organisation was co-operative with the Commission during its investigation and was prompt and forthcoming in its responses to queries posed by the Commission.
- (b) The Organisation took swift and extensive remedial action following the Incident.
- (c) The duration that the Compromised Personal Data was at risk was only for a limited time period. The Organisation was alerted to the Incident only a few days after the FTP port was opened to enable the VPN Workaround, and the Organisation took swift action thereafter to remove such access.
- (d) The VPN Workaround was only intended to be a temporary measure, and the Organisation had intended to revert to the use of the VPN. Thus, the potential for unauthorised disclosure of the Compromised Personal data would have been limited in any event.

17 Having considered the facts of this case and the factors outlined above, I hereby direct the Organisation to pay a financial penalty of \$5,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court³ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

3 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Learnaholic Pte Ltd

[2020] PDP Digest 387

Coram: Tan Kiat How, Commissioner

Case Number: DP-1703-B0567

Decision Citation: [2020] PDP Digest 387; [2019] SGPDPDC 31

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

26 August 2019

BACKGROUND

1 Learnaholic Pte Ltd (the “Organisation”) is an IT vendor that was providing attendance-taking and e-learning systems to schools pursuant to a contract with the Ministry of Education (“MOE”). The central issue to this case, in so far as it is related to the Personal Data Protection Act 2012¹ (“PDPA”), is whether the Organisation had made reasonable security arrangements to protect the personal data of approximately 47,802 students, students’ parents and staff of various schools that it had in its possession and control at the material time.

MATERIAL FACTS

2 The Organisation was responsible for the maintenance and installation of the attendance-taking system installed in [redacted] (“the School”). The School’s attendance-taking system was designed such that the attendance records would be updated each time a student “taps in” with his or her student pass at any one of the card readers located around the School. This attendance-taking system consisted of an attendance server (the “Attendance Server”) connected to clusters of attendance controllers

1 Act 26 of 2012.

linked to card readers. One such cluster was located at the guard post of the School (the “Guard Post Cluster”).

3 In or around March 2016, the School informed the Organisation of an intermittent problem with the Guard Post Cluster: students’ names were not being displayed despite their tapping in at the Guard Post Cluster. In order to investigate into the issues reported by the School, the Organisation decided to troubleshoot the problem remotely as this was more convenient than sending someone down to the School. In order to do so, it installed VNC Server, a remote desktop software, at the Guard Post Cluster; it used VNC Viewer to remotely connect to the VNC Server so that the Organisation would be able to troubleshoot the Guard Post Cluster without having to be physically present at the School (the “Remote Troubleshooting” method).

4 In addition to installing the VNC Server, the Organisation also took the following steps to facilitate its Remote Troubleshooting:

- (a) Modifying the configuration of the School’s Intranet firewall by opening a specific port (“Port”) to allow external access to the Guard Post Cluster from the Internet via the VNC Viewer software.
- (b) Disabling the password for the VNC Server software installed at the Guard Post Cluster (*ie*, no password was required to gain access to the Guard Post Cluster via the VNC Server software). While the Organisation claimed to have disabled the input feature at the client side when using the VNC Viewer program, this would have only affected the Organisation’s ability to make changes and would not have affected a hacker’s ability to do the same. If the Organisation had disabled the input feature at the server side, it would have been very unlikely that a hacker could have exploited the vulnerability in the Organisation’s system as explained immediately below. The only other potential manner in which the hacker could have exploited the said vulnerability would have been where the Organisation opened all the ports to the system instead of just the VNC specific port.

5 The Organisation’s actions would come to have significant consequences. Prior to the opening of the Port, the Guard Post Cluster was only accessible internally from the School network. The opening of the Port was meant to be temporary for the purposes of the Remote

Troubleshooting, but the Organisation's representative (the "Representative") conducting the troubleshooting forgot to close the Port and restore the School's original firewall configuration after the troubleshooting was completed. The disabling of the password for the VNC Server software meant that access to the Guard Post Cluster could be easily gained simply with knowledge of the Port number and the IP address of the Attendance Server. This combination of actions led to the creation of a vulnerability in the School's Guard Post Cluster (the "Vulnerability") – a vulnerability that would later be exploited by a hacker.

6 The Organisation took the view that the hacker exploited the Vulnerability to retrieve a configuration file stored on the Guard Post Cluster. The Commissioner believes that this is a logical explanation of how the hack occurred. This configuration file was supposed to be stored only on the School's Attendance Server but had inadvertently been copied to the Guard Post Cluster. This had occurred as the Organisation had stored the configuration file in a folder on the Attendance Server that also held firmware update files for the Guard Post Cluster (the "Update Folder"); the Update Folder would be periodically synced with the relevant components of the Guard Post Cluster in the School in order to "push down" firmware updates from the Attendance Server to these components at the Guard Post Cluster. A copy of the configuration file was therefore copied to the Guard Post Cluster during one of the periodic firmware updates.

7 The purpose of the configuration file was to enable the School's Attendance Server (using the Representative's work e-mail as a relay) to send attendance reports to the School's staff. To facilitate this function, the configuration file contained the login credentials of the Representative's work e-mail. The hacker was thus able to obtain the login credentials from the copy of the configuration file retrieved from the Guard Post Cluster, and thereby gain access to the Representative's work e-mail account. The Representative's work e-mail account contained the unencrypted personal data of approximately 47,802 staff, students and students' parents of various schools (the "Personal Data"). The Personal Data exfiltrated by the hacker included information such as:

- (a) names;
- (b) NRIC numbers;
- (c) contact numbers;
- (d) e-mail addresses;

- (e) addresses; and
- (f) medical information, which related to approximately 372 students.

8 The Personal Data was in the Representative's e-mail as the Organisation had assisted the schools to upload the data onto the respective schools' attendance taking and/or e-learning systems. The Representative had received the Personal Data via e-mail for the purposes of uploading but had not deleted these e-mails after performing the upload as it was thought that it might be useful to retain the Personal Data for future reference.

9 The breach of the School's attendance-taking system and the Representative's work e-mail, together with the resulting exfiltration of the Personal Data, were only discovered in February 2017 by the Singapore Police Force ("SPF") in the course of investigating a separate hacking incident.² The Personal Data Protection Commission ("PDPC") was informed of the matter and thereafter commenced its own investigations.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

The relevant Personal Data Protection Act 2012 provisions

10 In respect of this matter, the relevant provision is s 24 of the PDPA. 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 (the "Protection Obligation").

Preliminary issues

11 It is not disputed that the Personal Data is "personal data" as defined in s 2(1) of the PDPA. There is no question or dispute that the Organisation falls within the PDPA's definition of an "organisation". There is also no dispute that the Personal Data was, at all material times, in the

2 This hacking incident, and the Singapore Police Force's investigations, are not the subject of these grounds of decision.

Organisation's possession and that the Organisation was responsible for the Personal Data.

12 In the course of investigations, it was determined that the Organisation was at all material times an independent third-party service provider to, and therefore was not acting on behalf of, MOE or any of the various schools it provided IT services to. The Organisation also did not raise the applicability of s 4(1)(c) of the PDPA at any time. In the circumstances, s 4(1)(c) of the PDPA does not apply.

13 The key issue is therefore whether the Organisation had protected the Personal Data in its possession by making reasonable security arrangements to prevent unauthorised access and similar risks.

The Organisation failed to make reasonable security arrangements

14 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, the Commissioner is of the view that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession, and has thereby breached the Protection Obligation under s 24 of the PDPA. This data breach incident occurred due to a series of lapses on the part of the Organisation, all of which could have been reasonably averted.

15 First, the Organisation opened a Port and reconfigured the School's Intranet firewall to allow remote access to the School's Guard Post Cluster, while simultaneously disabling the password for remote access to the Guard Post Cluster, thereby creating the Vulnerability. In addition, the Representative conducting the Remote Troubleshooting forgot to close the Port, leaving the Vulnerability exposed from March 2016 until end-April 2016, when the Vulnerability was discovered because the Organisation was subsequently requested to troubleshoot the Guard Post Cluster again in or around April 2016.

16 It bears noting that the Organisation did not inform the School that it had made changes to the configuration of the School's Intranet firewall during the Remote Troubleshooting. The changes made to the configuration of the Intranet firewall in this matter was a clear security lapse borne of convenience; in attempting to get around the need to be physically present in the School, the Organisation undermined the security arrangements in place and allowed the hacker to obtain the configuration

file. This was exacerbated by the Organisation's failure to inform the School of these configuration changes.

17 Second, the configuration file (containing the login credentials of the Representative's work e-mail account) was supposed to be stored only in the School's Attendance Server. As described at [6] above, this configuration file had been inadvertently copied to the Guard Post Cluster, where the Vulnerability existed as a point of entry for the hacker, which allowed the hacker to consequently gain access to the configuration file.

18 The hacker was thus able to obtain the login credentials of the work e-mail account where the unencrypted Personal Data was stored. The Organisation has represented to PDPC that the e-mail accounts and passwords contained in the configuration file were listed in a jumbled up or random manner, such that it would not have been apparent which e-mail account corresponded with which password. Such an approach falls far below the level of sophistication which one would expect login credentials to be secured with. A relatively low degree brute-force attack (*ie*, trial and error) would be all that was required to match an e-mail account with its corresponding password. The Organisation failed to appreciate the consequences of placing the configuration file with the login credentials – a file that effectively contained the proverbial keys to the kingdom – in the Update Folder of the Attendance Server. Allowing a file that contained sensitive information such as login credentials to be copied to each of the clusters represents a clear lapse in the Organisation's security arrangements. The less-than-secure manner in which the login credentials were stored and dealt with within their own system was an issue that the Organisation should and could have been reasonably alive to.

19 Third, the Personal Data was sent to and stored in the Representative's work e-mail account in an unencrypted form. PDPC encourages the encryption of personal data that is sensitive or when sent in bulk. As this case demonstrated, personal data sent in bulk was stored in the clear in the Representative's e-mail account, effectively giving the hacker free rein to access the information once access to the e-mail account was obtained. The originator of the Personal Data shared some of the blame in failing to encrypt the file. But the risks would not have materialised had the Representative deleted the e-mail containing the Personal Data once his task was completed (*eg*, uploading of data). This he failed to do. He kept the e-mail containing the Personal Data, just in case he needed it in the

future. If there was a valid legal or business purpose for retaining a copy of the Personal Data for an extended period of time, it should not have been retained in the Representative's work e-mail account in an unencrypted format. The Organisation could have downloaded a copy of such data into a computer and encrypted the same if it needed to retain it (and thereafter deleting the originating e-mail and attachment). This is a basic security arrangement that could have been reasonably expected of the Organisation.

20 The Organisation's inadequate security measures were therefore directly responsible for the breach and exfiltration of the Personal Data. Any of the individual lapses on their own would have been a cause for concern; combined together, the lapses created the perfect opportunity for any opportunistic hacker armed with basic hacking tools to strike.

21 Based on the foregoing, the Commissioner finds that the Organisation has breached the Protection Obligation under s 24 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

22 Having found the Organisation to be in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

23 In determining the appropriate directions to be imposed on the Organisation, the Commissioner has taken into account the following aggravating factors:

- (a) In the course of its work with the schools and MOE, the Organisation was handling large volumes of personal data relating to minors, including sensitive personal data such as their medical information, family structure and NRIC numbers. The unauthorised disclosure of such data could potentially have caused significant harm.

- (b) The Vulnerability was left unattended for a period of more than a month during which other hackers could have easily obtained access to the Personal Data.³
- (c) Actual data exfiltration had taken place.

24 To its credit, the Organisation acted fairly swiftly to address the causes of the breach once it was made aware of the same, a response which carries some mitigating value. The following remedial actions taken by the Organisation have therefore been taken into account:

- (a) changed the passwords for all the Organisation's work e-mail accounts;
- (b) activated two-factor authentication for all of the Organisation's work e-mail accounts after being informed of the data breach by SPF;
- (c) deleted all e-mails with the Personal Data from the Organisation Representative's work e-mail account;
- (d) deleted the configuration file from the Guard Post Cluster;
- (e) implemented a new practice of having the Organisation's representatives delete e-mails from their work e-mail account once action has been taken in respect of the same; and
- (f) put in place a script to ensure that the Update Folder of the Attendance Server only contains essential php files such as system codes, and that any non-essential files are automatically deleted prior to the syncing of the Update Folder with the other attendance clusters in the School.

The Organisation's representations

25 The Organisation made representations to PDPC, in particular to reduce the quantum of the financial penalty imposed, after the preliminary decision was issued to the Organisation. The Organisation's representations are addressed as follows.

26 First, the Organisation represented that the total number of individuals affected was 35,000 (and not 60,000 according to initial

3 During the investigations, there had been some uncertainty as to the duration for which the Vulnerability was left uncorrected. This is further discussed at [27] below.

calculations), and that the total number of students whose medical data was accessed and exfiltrated was 372. PDPC has reviewed the evidence and determined that the number of unique individuals affected by the incident was 47,802. The Commissioner accepts that 372 individuals' medical data was accessed. The financial penalty has, therefore, been adjusted to take into account the number of individuals whose medical data was accessed and exfiltrated and the reduction in the number of affected individuals.

27 Second, the Organisation represented that the Vulnerability had been discovered and fixed sometime at the end of April 2016 when the Organisation was requested to troubleshoot the Guard Post Cluster again (as described at [15] above). The Organisation had previously indicated that it was unaware of the duration during which the Vulnerability was left uncorrected. In the circumstances, the financial penalty quantum was initially based on the Vulnerability having only been corrected on or about February 2017 when the Organisation was notified of the incident by SPF in the course of investigating a separate hacking incident. The Commissioner has given the Organisation the benefit of the doubt as to the period of time the Vulnerability existed and has adjusted the quantum of the financial penalty accordingly.

28 Third, the Organisation also represented that the medical information subject to unauthorised access relates to types of medical conditions⁴ which it asserts are non-sensitive in nature. However, the medical data that was accessed was those of minors, *ie*, less than 21 years of age. Medical data and personal data of minors are treated as being sensitive in nature.⁵ For such sensitive personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.

29 Fourth, the Organisation represented that it had requested the schools to upload personal data on their own, to limit any personal data sent to the Organisation to what is absolutely necessary, and if the schools were to send data via e-mail, to password protect the data file attachments. However, the

4 For instance, colour vision; whether the student was on regular medication; respiratory disorders; allergies; asthma; epilepsy; heart condition; ear disorder; hearing loss; periodic loss of consciousness; and modified exercise.

5 See *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* at para 8.12 and *Re Singapore Taekwondo Federation* [2019] PDP Digest 247 at [22]–[27].

preferred practice of many of the schools was to send unencrypted personal data to the Organisation for it to be uploaded. To give the Organisation the benefit of the doubt, even if it is accepted that the Organisation had informed the schools to password protect data file attachments sent by e-mail, the evidence shows that this policy was not observed in practice. Merely having a policy is not a sufficient security arrangement, particularly when this policy is observed only in its breach.

30 As a corollary to the above point, the Organisation also represented that “as a vendor and a small enterprise serving the educational institutions, [the Organisation was] understandably subservient to the decisions of their customers”. If the Organisation chooses to accede and upload the personal data that was sent to its e-mail account, then it ought to have reviewed its policies and implemented different security arrangements to protect such personal data, *eg*, by deleting file attachments containing personal data promptly.

31 Fifth, the Organisation represented that its practices were to delete e-mails containing personal data when no longer required (*eg*, after uploading to the appropriate databases), and that the reason that the attacker was able to gain access to so many e-mail attachments containing Personal Data is because he had access to the e-mail account for three months. While this may be true, the Organisation previously admitted that e-mails containing Personal Data would still be required to address enquiries from schools, and thus, were retained in the Representative’s e-mail account for months (and not immediately deleted after uploading). As stated at [19] above, the fact that the Personal Data was retained in such a manner facilitated the hacker’s access to the Personal Data; if the Organisation needed to keep the Personal Data for operational purposes, it should have properly secured it.

32 Sixth, the Organisation represented that the following should be taken into account as mitigating factors:

- (a) it was a victim of a cyberattack that had maliciously exploited the lapses on the part of the Organisation;
- (b) the Organisation tried its even best to secure personal data, but its lone efforts were insufficient without reciprocation from the schools; and

- (c) based on SPF's investigations there was no evidence of further exploitation, use or disclosure of the Personal Data by the attacker.

33 With respect to [32(a)], it should be reiterated that being a cyberattack victim is not in itself a mitigating factor, especially in this case where the lapses of the Organisation, including the existence of the Vulnerability, were such that the attacker would not require sophisticated means to obtain unauthorised access to the Personal Data.

34 Paragraph [32(b)] has been addressed above.⁶ With respect to [32(c)], while there was actual exfiltration of the Personal Data in this case,⁷ there was no evidence of further exploitation, use or disclosure of the Personal Data by the attacker. This has been taken into account in the revised financial penalty.

35 Finally, the Organisation also sought to compare the penalty imposed against it with that of previous cases.⁸ However, the cases cited dealt with identification data while this case involved medical data of minors. The Commissioner is satisfied that the financial penalty imposed in this case is justified, in particular given the aggravating factors set out above at [23].

36 Having considered all the relevant factors of the case, the Commissioner hereby directs the Organisation to pay a financial penalty of \$60,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court⁹ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

6 See [29] and [30] above.

7 This has been taken into account as an aggravating factor: see [23(c)] above.

8 Specifically, *Re K Box Entertainment Group Pte Ltd* [2017] PDP Digest 1, *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 and *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223.

9 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re O2 Advertising Pte Ltd

[2020] PDP Digest 398

Coram: Tan Kiat How, Commissioner

Case Number: DP-1807-B2376

Decision Citation: [2020] PDP Digest 398; [2019] SGPDPDC 32

Accountability Obligation – Lack of data protection policies and practices – Failure to appoint data protection officer

Protection Obligation – Unauthorised disclosure of personal data – Insufficient 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

28 August 2019

BACKGROUND

1 An individual found some of his personal data accessible on the Internet without his consent. In particular, the individual found that when he conducted a search on Google using his name and NRIC number, the search results included a URL link (the “URL Link”) to a database maintained by O2 Advertising Pte Ltd (the “Organisation”). The database contained the personal data of numerous individuals including the individual’s (the “Affected Individuals”). On 10 July 2018, the individual lodged a complaint with the Personal Data Protection Commission (“Commission”) over the incident.

MATERIAL FACTS

2 The Organisation provides advertising and marketing services in Singapore. In 2015, the Organisation collected the Affected Individuals' personal data during an advertising campaign conducted on behalf of one of its clients. The Organisation stored the collected personal data in two databases.

3 The incident resulted in the following types of personal data of the Affected Individuals being either exposed to unauthorised access or at risk of unauthorised access (the "Disclosed Data") depending on which database the Disclosed Data was stored in:

- (a) name;
- (b) NRIC number;
- (c) e-mail address;
- (d) residential address;
- (e) gender;
- (f) date of birth;
- (g) mobile number;
- (h) age; and
- (i) skin type.

4 The Disclosed Data of 403 Affected Individuals was stored in one database ("Database A") and exposed to unauthorised access through the URL Link found by the complainant. The Disclosed Data of 1,165 Affected Individuals was stored in another database ("Database B") which was at risk of unauthorised access. This was because after accessing Database A using the URL Link, a party with knowledge of how to navigate the root directory could possibly gain access to Database B. In addition, there was a risk of unauthorised access to two php files found in a directory containing user names and passwords to the Organisation's e-mail system and another database ("Exposed Credentials"). Using the same URL Link, a party with knowledge of how to navigate the root directory could also possibly gain access to the Exposed Credentials.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

5 The issues for determination are:

- (a) whether the Organisation breached the Protection Obligation under s 24 of the Personal Data Protection Act 2012¹ (“PDPA”);
- (b) whether the Organisation complied with its Retention Limitation Obligation under s 25 of the PDPA; and
- (c) whether the Organisation complied with its Accountability Obligation under ss 11(3) and 12 of the PDPA.

Whether the Organisation breached section 24 of the Personal Data Protection Act 2012

6 Databases A and B which contained the Disclosed Data were maintained by the Organisation. Hence, the Organisation had possession and control of the Disclosed Data at all material times and therefore had an obligation to protect them. Database A was in the Public_HTML directory of a server and was not secured with any form of access controls. This enabled Internet search engines like Google to index the URL Link to Database A, resulting in it showing up in search results. As stated above, this also exposed Database B to risk of unauthorised access. The Organisation asserted that the server hosting Database A and Database B was password protected. However, this was not a security arrangement to restrict access to the databases which had been stored in the Public_HTML directory.

7 As observed in *Re Tutor City*,² there are a number of technical security measures that can be implemented to prevent documents from being indexed by web crawlers:

- (a) First, the Organisation could have placed these documents in a folder of a non-public folder/directory.
- (b) Second, the Organisation could have placed these documents in a folder of a non-public folder or directory, with access to these documents being through web applications on the server.

1 Act 26 of 2012.

2 [2020] PDP Digest 170 at [21]–[23].

- (c) Third, the Organisation could have placed these documents in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (eg, implement a password requirement or an IP address restriction).

8 Since its website went live over five years ago, the Organisation had not conducted any vulnerability scanning. The flaws in the security of its website that had been discovered during investigations would have been revealed in a vulnerability scan. Had one been conducted, the Organisation would have been in a position to put in place reasonable security arrangements mentioned in the preceding paragraph.

9 For the reasons above, the Commissioner finds the Organisation in breach of s 24 of the PDPA.

Whether the Organisation breached section 25 of the Personal Data Protection Act 2012

10 Under s 25 of the PDPA, an organisation is obliged to cease retaining personal data once the purpose for which the personal data was collected has been served, unless further retention can be justified for legal or business purposes. The Organisation admitted that it had overlooked deleting the Disclosed Data and that there were no reasonable grounds to continue retaining them after the engagement with its client ceased in 2016. The Disclosed Data was only deleted by the Organisation after it was informed by the Commission of the complaint. The Commissioner therefore finds the Organisation in breach of s 25 of the PDPA.

Whether the Organisation breached sections 11(3) and 12 of the Personal Data Protection Act 2012

11 Section 11(3) of the PDPA requires the Organisation to appoint a data protection officer; s 12 of the PDPA imposes an obligation on organisations to develop and implement data protection policies and practices. The Organisation admitted that at the material time, it did neither of these. In the circumstances, the Commissioner finds that the Organisation failed to meet its obligations under ss 11(3) and 12 of the PDPA.

REPRESENTATIONS BY THE ORGANISATION

12 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose. In the beginning of 2016, the Organisation discovered it was a victim of a fraud involving the misappropriation of company funds amounting to approximately \$3.2m, resulting in massive retrenchment and significant cash flow issues for the Organisation. Consequently, the Organisation's financial performance for the past few years has been weak, and it is currently in dire financial straits. The director is 72 years old and is the Organisation's sole employee since 1 March 2018. He intends to continue the Organisation's business on a significantly reduced scale.

13 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to \$10,000. The quantum of financial penalty has been determined after due consideration of the Organisation's finances and to avoid imposing a crushing burden on the Organisation given its present financial circumstances and future prospects. Although a lower financial penalty has been imposed in this case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

THE COMMISSIONER'S DIRECTIONS

14 Having found the Organisation in breach of ss 11(3), 12, 24 and 25 of the PDPA, the Commissioner hereby directs the Organisation:

- (a) 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 Court³ in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full;
- (a) to appoint an individual responsible for ensuring the Organisation's compliance with the PDPA within 30 days from the date of the Commissioner's direction;
- (a) to develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the

3 Cap 322, R 5, 2014 Rev Ed.

PDPA within 60 days from the date of the Commissioner's direction; and

- (a) to inform the Commission of the completion of each of the above directions in (b) and (c) within one week of implementation.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Amicus Solutions Pte Ltd and another

[2020] PDP Digest 404

Coram: Tan Kiat How, Commissioner

Case Number: DP-1610-B0290

Decision Citation: [2020] PDP Digest 404; [2019] SGPDPDC 33

Consent Obligation – Notification obligation – Unauthorised sale of personal data

Consent Obligation – Notification obligation – Unauthorised use of personal data

Continued disclosure of personal data collected before appointed day

30 August 2019

1 The Personal Data Protection Commission (the “Commission”) received a complaint regarding the unauthorised collection and use of personal data to market financial products. Investigations were commenced into the alleged unauthorised sale and disclosure of personal data by a data broker and the unauthorised collection and use of the personal data for telemarketing purposes. Upon conclusion of investigations and consideration of the totality of evidence, the Commissioner found Amicus Solutions Pte Ltd (“Amicus”) and Mr Ivan Chua Lye Kiat (“Mr Chua”) to be in breach of the Personal Data Protection Act 2012¹ (“PDPA”) for the reasons set out in these grounds.

MATERIAL FACTS

2 An independent life insurance brokerage company (the “Insurance Brokerage”) appointed Mr Chua as a financial adviser director to provide financial advisory services and to market financial products distributed by the Insurance Brokerage to prospective clients in accordance with the terms set out in a “Financial Adviser Representative Agreement”. He oversees a

1 Act 26 of 2012.

team of financial adviser representatives. Their main products are Eldersfield-related insurance policies targeted at individuals over 40 years old.

3 It is undisputed that Mr Chua and the financial adviser representatives in his team are not employees of the Insurance Brokerage but independent agents. As independent agents, they receive a commission for each sale but are not in an employer-employee relationship with the Insurance Brokerage nor are they entitled to any employee benefits such as employer Central Provident Fund contributions and/or medical benefits.

4 One of Mr Chua's primary roles as a financial adviser director is to seek out new customers. Mr Chua mainly relied on referrals from existing customers, but he also engaged telemarketers to make cold calls to potential customers. These telemarketers are independently sourced with no assistance of or referrals from the Insurance Brokerage; telemarketers are directly engaged by Mr Chua or the financial adviser representatives in his team.

5 Amicus is an organisation that provides business and consultancy management services and claims to be able to provide business opportunities and marketing plans with its database. It claims to have 1.8 million contacts which it markets as being in compliance with the PDPA and the Personal Data Protection (Do Not Call Registry) Regulations 2013.² Aside from the sale of data, Amicus also offers a range of services such as purchasing property ownership information (including caveats) on behalf of property agents, data mining and Do Not Call ("DNC") Registry scrubbing services.

6 During investigations, Mr Chua was upfront in admitting that he had purchased telemarketing leads from Amicus both before and after 2 July 2014, the date when Pts III to VI of the PDPA ("Data Protection Provisions") came into effect (the "Appointed Day"). Mr Chua represented that before the Appointed Day, Amicus sold personal data (including the individual's name, mobile number, gender and birthday) at \$0.50 to \$1 per record. After the Appointed Day, the products that were offered by Amicus changed. The previous product was no longer offered but it now offered different products. For Mr Chua's commercial purposes, the product that

2 S 709/2013.

he was interested in was the sale of telephone numbers of individuals above 40 years old (which was his team's target demographic), each of which was sold for between \$0.01 and \$0.02.

7 Mr Chua provided two datasets that he claimed to have purchased from Amicus after the Appointed Day. The information disclosed in these datasets is set out in the table below:

	Information Disclosed	Number of Records in the List
List 1	<ul style="list-style-type: none"> • partial NRIC number, <i>ie</i>, the first four digits (for some entries); • partial date of birth (for those that did not include a partial NRIC number);³ • gender; and • mobile phone number 	11,384
List 2	<ul style="list-style-type: none"> • partial NRIC number, <i>ie</i>, the first four digits (for some entries); • partial date of birth; • gender; and • mobile phone number 	10,074

8 Telemarketers engaged by Mr Chua and his team relied on the information in these datasets to help generate leads and sales for the team by making cold calls to the individuals in the datasets. Mr Chua informed the Commission that Amicus had sold both Lists 1 and 2 to him and confirmed that he did not purchase such lists from any other source at the time. While Amicus admitted that it sold Mr Chua two datasets, it disputed Mr Chua's account that both Lists 1 and 2 were sold to him after the Appointed Day. By Amicus' account, it only sold Mr Chua one dataset after the Appointed Day though it was unable to identify which of the two lists (*ie*, Lists 1 and 2) it had sold to Mr Chua.

9 Amicus also admitted to selling the following dataset to another individual on another occasion after the Appointed Day at \$0.10 per record in the course of the investigations:

3 Amicus admitted that the information it sold to Mr Chua included partial NRIC numbers (*ie*, the first four digits) but denied that the information contained the individuals' dates of birth.

	Information Disclosed	Number of Records in the List
List 3	<ul style="list-style-type: none"> • age; • gender; and • mobile phone number 	1,200

10 However, Amicus denied any wrongdoing in selling the datasets with the type of personal data found in Lists 1, 2 and 3 (the “datasets”) as it contended that the information in the datasets was not personal data to begin with. It also argued that the information in the datasets was publicly available data that it collected from public sources such as the *Government Gazette* and records of the Singapore Land Authority (“SLA”) and the Accounting and Corporate Regulatory Authority (“ACRA”), and the information in the datasets was collected before the Data Protection Provisions came into effect on the Appointed Day.

11 During investigations, Amicus was unable to give a satisfactory explanation regarding the source of the information in the datasets. Investigations were not able to establish with any degree of certainty when the lists were compiled or obtained, nor where the lists were sourced from. [Redacted] (replaced with “Mr L”), who is in charge of the day-to-day operations of Amicus, gave evidence on behalf of Amicus and initially claimed that the personal data was obtained from publicly available sources. However, he subsequently claimed that the personal data was obtained from organisers of surveys, meetings and seminars as well as call centres but was unable to name any of the seminars or meetings from which Amicus had purportedly collected the information or the organisations that conducted the surveys or operated the call centres when queried. Thereafter, he claimed that the personal data was obtained from telemarketing and multi-level marketing (“MLM”) companies, though he was again unable to name any of these companies, nor provide any proof of purchase. Finally, upon further questioning, Amicus represented that the information in the datasets was actually collected before the Appointed Day. He confirmed that he did not collect personal data found in the datasets from publicly available sources.

Number of datasets sold

12 As a preliminary issue, while Amicus and Mr Chua disagreed over the number of datasets that Amicus sold Mr Chua after the Appointed Day,⁴ an evaluation of the evidence in its entirety shows Mr Chua's evidence to be more credible for the following reasons:

- (a) Mr Chua offered the two lists that he claimed to have purchased from Amicus after the Appointed Day even though it was to his detriment. The Commission had commenced investigations on the basis of information provided by a complainant who had requested for anonymity. At the time Mr Chua volunteered the two lists, he was only aware that a complaint had been made against him but was not aware of the information which was provided to the Commission. Hence, the fact that he volunteered information that he knew could be detrimental to himself spoke to his openness and willingness to co-operate with investigations.
- (b) Although both lists were not dated and he was unable to produce any receipts, Mr Chua was able to produce a screenshot of an e-mail dated 22 March 2016 containing List 1 from one [redacted] (replaced with "Mr N") from Amicus.
- (c) Both Lists 1 and 2 only contain partial NRIC numbers, partial dates of birth, gender and mobile phone numbers. They did not contain names of the individuals. The evidence is that Amicus only started selling lists without names after the PDPA came into effect. Before the PDPA came into effect they sold lists with full names and these lists were more valuable than those sold after the PDPA came into effect. Given that Lists 1 and 2 do not contain full names, it is more likely than not that both these lists were sold after the PDPA came into effect.
- (d) Mr Chua was very co-operative throughout the investigation and there was no evidence to suggest that he had been anything less than forthcoming.

13 In contrast, as described at [11] above, Amicus had prevaricated during investigations and was unable to give a satisfactory explanation regarding the source of the information in the datasets and was unable to

4 See [8] above.

provide any documentary evidence on the dates Lists 1 and 2 were sold. Further, Amicus appeared to have intentionally limited the documentary trail in respect of the sale of Lists 1 and 2. According to Mr Chua, despite allowing its clients, including Mr Chua, to pay for its DNC scrubbing services by cheque, Amicus required cash payment for the lists. Amicus confirmed that it required Mr Chua to pay cash. It is suspicious that a company that has two commercial transactions with the same customer will allow payment for one by cheque but require payment by cash for the other. This conduct is less than straightforward. The reason provided by Amicus for requiring cash payment was that Amicus needed Mr Chua to verify the data in person. The reason provided does not in any way explain why Amicus could not accept cheque payments from Mr Chua when he collected the lists in person.

14 For the foregoing reasons, the following assessment is based on Mr Chua's evidence that Amicus had sold him two datasets (*ie*, Lists 1 and 2) after the Appointed Day.

FINDINGS AND BASIS FOR DETERMINATION

15 The issues for determination are:

- (a) whether the information disclosed in the lists constituted personal data;
- (b) whether Amicus had collected, used and/or disclosed personal data without consent and/or notification; and
- (c) whether Mr Chua used and/or disclosed the personal data without consent and/or notification.

Whether the information disclosed constituted personal data

16 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.

17 The information disclosed in all three datasets are as follows:

	Information Disclosed	Number of Entries in the List
List 1	<ul style="list-style-type: none"> • partial NRIC number, <i>ie</i>, the first four digits (for some entries); • partial date of birth (for those that did not include a partial NRIC number);⁵ • gender; and • mobile phone number 	11,384
List 2	<ul style="list-style-type: none"> • partial NRIC number, <i>ie</i>, the first four digits (for some entries); • partial date of birth; • gender; and • mobile phone number 	10,074
List 3	<ul style="list-style-type: none"> • age; • gender; and • mobile phone number 	1,200

18 As mentioned at [11] and [12] above, although Amicus admitted that it sold datasets containing individuals' mobile phone numbers, age range and gender, it contended that no personal data was disclosed in the datasets because it was "sufficiently anonymised". The datasets did not disclose the individual's name, NRIC number, address or any unique personal information but only included truncated NRIC numbers (*ie*, only the first four digits) and dates of birth (*ie*, only the month and year of birth).

19 There are certain types of information that are unique identifiers, which are capable of identifying an individual in and of themselves. The *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* set out a non-exhaustive list of information that the Commission generally considers to be unique identifiers:⁶

5 Amicus admitted that the information it sold to Mr Chua included partial NRIC numbers (*ie*, the first four digits) but denied that the information contained the individuals' dates of birth.

6 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* at para 5.10.

- (a) full name;
- (b) NRIC number or FIN (foreign identification number);
- (c) passport number;
- (d) *personal mobile telephone number*;
- (e) facial image of an individual (*eg*, in a photograph or video recording);
- (f) voice of an individual (*eg*, in a voice recording);
- (g) fingerprint;
- (h) iris image; and
- (i) DNA profile.

20 In *Re My Digital Lock Pte Ltd*,⁷ the Commission observed that information will generally only be considered to be a unique identifier if there is a one-to-one relationship between the information and the individual, *ie*, the information is not typically associated with more than one individual:

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* ('Key Concepts Guidelines') at para 5.10 provides a list of information that is considered to be capable of 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).* [emphasis added; footnote omitted]

21 The lists were sold for the purpose of generating leads for the sale of Eldersfield and other personal insurance policies. A natural inference is that the mobile numbers in the lists were *personal* mobile numbers. As a personal mobile phone number is generally tied to an individual subscriber who uses it as his or her individual contact number to the exclusion of others, it is *prima facie* personal data given its one-to-one relationship.

22 The "redacted" or truncated NRIC numbers in the datasets do not conform to the Commission's published advisory guidelines on redaction of

7 [2018] PDP Digest 334 at [11].

NRIC numbers which are designed to minimise the risk of re-identification. On the contrary, the key piece of information that the “redacted” NRIC number was intended to convey was the age of the person that it is associated with given that it is well known that the first four digits of the NRIC discloses the year of registration (and accordingly, the age) of the individual. It is trite that NRIC numbers are the same as birth certificate numbers that are assigned upon registration of birth, which has to take place within x days or weeks of birth. Hence, there was every intention to convey information about the year of birth of the individual associated with the personal mobile phone number.

23 Accordingly, although the information disclosed in the datasets did not include the names of the individuals, the information is still personal data as defined in s 2(1) of the PDPA because the individuals in Lists 1 and 2 were identifiable directly or indirectly through their year of birth and personal mobile numbers.

24 Likewise, the individuals in List 3 were directly identifiable through their personal mobile phone numbers.

Whether the Organisations breached section 13 and/or section 20 of the Personal Data Protection Act 2012

25 As the PDPA defines “organisation” to include “any individual, company, association or body of persons, corporate or unincorporated”, each of Mr Chua and Amicus is an organisation under the PDPA. As mentioned in *Re Spring College International Pte Ltd*,⁸ the PDPA adopts a consent-first regime and the concepts of notification of purpose and consent are closely intertwined. Pursuant to s 13 of the PDPA, unless an exception to consent is applicable, organisations are generally required to obtain the consent of an individual before collecting, using and/or disclosing the individual’s personal data (“Consent Obligation”). Consent must be obtained from the individual with reference to the intended purpose of the collection, use or disclosure of the personal data. The organisation’s collection, use and disclosure of personal data are limited to the purposes for which notification has been made to the individuals concerned. In this regard, organisations have an obligation under s 20 of

8 [2019] PDP Digest 230 at [10].

the PDPA to inform individuals of the purposes for which their personal data will be collected, used and/or disclosed, on or before collecting the personal data in order to obtain consent (“Notification Obligation”).

26 As observed in *Re Sharon Assya Qadriyah Tang*,⁹ the buying and selling of leads that comprise personal data of individuals are activities that fall under the scope of the PDPA:

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.* [emphasis added]

Amicus

27 As the organisation with possession and control in respect of the personal data in the datasets that it compiled and sold, Amicus has a duty to comply with the data protection obligations under the PDPA, specifically the Consent and Notification Obligations. However, Amicus contended that it was not necessary for it to obtain consent or to notify individuals before selling the datasets because, among other things:¹⁰

- (a) the information was collected before the Consent and Notification Obligations came into force; or
- (b) the information was publicly available.

28 As stated above, Amicus had been prevaricating during investigations without providing a clear and consistent explanation as to when and how the personal data in the lists were obtained, nor their source. Taking its case

9 [2018] PDP Digest 319 at [13].

10 Amicus also argued that it was not required to obtain consent and notify the individuals before selling the datasets because the information contained in the datasets are not personal data. We refer to our findings on this issue at [18]–[24] above.

at the highest, the following analysis takes each of these possible defences separately as each, if successful, can stand independently.

Personal data collected before the Appointed Day

29 One of Amicus' main defences was that the information in the datasets was collected before the Data Protection Provisions came into force and Amicus was therefore not subject to the Consent and Notification Obligations in relation to the personal data that it collected, used and/or disclosed. Section 19 of the PDPA allows organisations to 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 consent for such use is withdrawn. As such, it may be possible for an organisation to continue using personal data that was purchased or obtained before the Appointed Day without consent or notification if such use falls within the purposes of collection, provided that there was no indication that the individual did not consent to the continued use.¹¹

30 However, s 19 of the PDPA only covers the *use* of personal data collected before the Appointed Day and not the *disclosure* of personal data. As was held in *Re Sharon Assya Qadriyah Tang*, the grandfathering provision in s 19 of the PDPA would not apply to instances where the organisation had been selling personal data before the Appointed Day, and continued to sell personal data after the Appointed Day.¹²

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 was 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 Commission has stated this position in its Advisory Guidelines as an example:

11 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [20].

12 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [22] and [23].

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 was 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.

[emphasis added in bold italics]

31 Moreover, even if Amicus had collected the personal data before 2 July 2014, that permitted it to disclose by way of sale, it would have had to obtain fresh consent for such purposes of disclosure after the Appointed Date. Needless to say, Amicus was not able to provide evidence of either during the course of investigations. As mentioned at [11] above, Amicus was unable to satisfactorily explain the source of the personal data in the datasets. During the course of the investigation, Amicus first claimed that the information was collected from surveys, meetings and seminars, but subsequently represented that it was collected from telemarketing and MLM companies. Nevertheless, even if the individuals had provided their personal data during surveys or at meetings and seminars, or even if the personal data was collected from telemarketing or MLM companies, Amicus did not provide any evidence that the individuals concerned had provided fresh consent after the Appointed Date for their personal data to be disclosed by way of sale to telemarketers. In this regard, Amicus acknowledged that it could have sought consent given that it possessed the individuals’ full NRIC numbers and personal mobile phone numbers but conceded that it did not do so.

32 In the circumstances, there was a clear breach of the Consent and Notification Obligations under the PDPA in respect of Amicus’ sale of the datasets containing personal data after the Appointed Day.

Publicly available exception

33 The alternate defence that Amicus raised during the investigations, but which it subsequently dropped, was that the information in the datasets was publicly available information obtained from public sources, such as records of registered doctors, lawyers and engineers published in the *Government Gazette*, and records from SLA and ACRA. The PDPA sets out an exception for the collection, use and disclosure of personal data that is publicly available.¹³ However, by Amicus' own admission, the *Government Gazette* only contained the names and organisations of certain individuals, which did not form part of the information that was found in the datasets it sold after the Appointed Day.

Representations by Amicus and an affiliated company

34 Amicus and an affiliated company, Ilied.com Pte Ltd ("Ilied"), submitted written representations to the Commission (the "Representations") after Amicus received a copy of the preliminary decision. The Representations were signed off by Mr L. In the Representations, Ilied and Amicus raised the following three points:

- (a) Ilied was the organisation that sold the datasets, and not Amicus;
- (b) List 1 was transacted before the Appointed Day; and
- (c) the datasets did not contain personal data as they had been truncated and anonymised, and further, that personal mobile phone numbers are not personal data *per se*.

The identity of the organisation which sold the datasets

35 The Representations enclosed two invoices issued by Ilied in support of the assertion that it was Ilied which had sold the data (the "Invoices"). The first Invoice, for the sum of \$1,900, was dated 25 June 2014 and was issued for "Leads Born 1973, 1975". The second Invoice, for the sum of \$1,138, was dated 22 March 2016 and was issued for "Data Sales".

13 Paragraph 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).

36 Ilied is an affiliate of Amicus and together with Amequity Solutions Pte Ltd (“Amequity”), are part of a group of closely related companies managed by Mr L, with some of the shareholders and directors being common across the said affiliated companies.

37 The Commission has reviewed the Representations and the additional evidence and finds that on a balance of probabilities, Amicus sold the data.

38 Ilied attempted to use the Invoices as incontrovertible proof that it was Ilied, and not Amicus, which had sold the datasets. However, Mr L, Mr N and [redacted] (replaced with “Ms J”), the director and shareholder of Amicus, Ilied and other affiliated companies, stated in their statements to the Commission that Amicus, Ilied and all affiliated companies operated as a single entity, with no clear demarcation between the companies. The entire group of companies was, in effect, headed by Mr L. Ilied individually had no real function but was merely used “for receipt purpose”¹⁴ and it did not even have a bank account.¹⁵ The facts suggest that Ilied’s issuance of the Invoices was merely an administrative arrangement and that Ilied, in fact, did not engage in data sales.

39 Furthermore, Amicus’ vacillation in its responses to the Commission also suggests that Amicus’ new claim that Ilied was the data seller should be treated with circumspection. As noted at [52(d)] below, Amicus was inconsistent in its responses and kept changing its account of the facts. In particular, Amicus provided inconsistent accounts on the source of the personal data, initially claiming that it was collected from publicly available sources, subsequently claiming that it was collected from surveys, meetings and seminars, and finally claiming that it was collected from telemarketing and MLM companies. Amicus was also inconsistent in its statements concerning Amequity. Amicus stated in the Representations that Amequity “is not into data business, but credit collection by banks”. However, in the same Representations, Amicus also stated that one of the lists of personal data, dated 5 March 2014, had been sold by Amequity.

40 Amicus, through its representatives Mr N and Mr L, admitted initially that it was Amicus that sold the datasets. This was corroborated by Mr Chua. Mr N explained Ilied’s issuance of the receipt by stating that

14 Mr N’s statement dated 30 April 2019.

15 Mr L’s statement dated 30 April 2019.

Illed, like Amequity, had no real function but was used for “receipt purpose”. Mr L also admitted in his statement given on 3 February 2017 that “data selling is purely done by Amicus”. There is no reason to distrust the consistent evidence of all three individuals, reflected in separate statements recorded at different times.

41 Amicus subsequently tried to explain this away by saying that Mr L’s statement referred to above at [40] was made “with reference to the business done by Amicus vis-à-vis Amequity”, and that “the term Amicus was used loosely to refer to company that do data sales [*sic*]”. Amicus further claimed that it had “confused itself” to be the seller because the Commission’s Notice to Require Production of Documents and Information (“NTP”) was addressed to it. If it was true that both Amicus and Illed engaged in data selling, this would have been operative on Mr L’s mind when answering the NTP and at the very least raised the possibility that it may have been Illed which sold the data instead, earlier in the investigations. The fact that all three individuals, Mr N, Mr L and Mr Chua, were consistent in omitting to mention Illed during the investigations shows that it was only Amicus that was engaged in data sales. The reasonable explanation is that while the invoices may have been issued by other companies affiliated to Amicus, such as Illed or Amequity, it was Amicus that in fact engaged in data sales and Illed and Amequity’s part in the arrangement was to merely issue invoices.

42 For the above reasons, it is more likely than not that Amicus sold the data to Mr Chua. Accordingly, the assertion in the Representations that it was Illed which had sold the data cannot be accepted.

Date of transaction for List 1

43 Illed claimed that the first Invoice was a receipt for List 1, and as the first Invoice was dated 25 June 2014, List 1 was transacted before the Appointed Day. However, it is unlikely that the first Invoice was a receipt for List 1. The quantity reflected on the first Invoice is 19,000, whereas the quantity of records in List 1 was 11,384. On the facts, it is more likely that List 1 was transacted on 22 March 2016, *ie*, after the Appointed Day, for the following reasons:

- (a) As noted at [12(b)] above, Mr Chua was able to produce a screenshot of an e-mail from Mr N, containing List 1. The

- e-mail was dated 22 March 2016, which was the same as the date on the second Invoice.
- (b) The second Invoice, which was dated 22 March 2016, was more likely to be the receipt for List 1.
 - (c) Mr N corroborated in his statement that List 1 was sold on 22 March 2016.
 - (d) List 1 contained personal data of individuals born in 1976 whereas the first Invoice was issued for “Leads Born 1973, 1975”.
 - (e) The second Invoice reflected a quantity of 11,380, which was closer to the quantity of records in List 1 than the quantity reflected in the first Invoice.
 - (f) As noted at [18] above, List 1 contained truncated personal data. As noted at [45] below, the truncation had apparently been done in an attempt to comply with the requirements of the PDPA and, as such, List 1 was more likely to have been transacted after the Appointed Day.

44 In view of the above factors, the weight of the evidence points to the fact that List 1 was transacted after the Appointed Day.

Whether the datasets contained personal data

45 In the Representations, Ilied claimed that it sought to comply with the requirements of the PDPA by truncating and anonymising the personal data. As noted at [22] above, the “redacted” or truncated NRIC numbers in the datasets do not conform to the Commission’s published advisory guidelines on redaction of NRIC numbers. The “redacted” NRIC numbers were intended to, and did in fact, convey information about the year of birth of the individual associated with the personal mobile phone number.

46 Ilied further claimed in the Representations that its research showed that an individual’s mobile phone number is *likely* to be personal data as it *may* be uniquely associated with an individual, but stopped short of admitting that all mobile phone numbers were personal data. In this regard, Ilied has not raised any evidence or arguments to suggest that the personal mobile phone numbers disclosed in the datasets were not personal data. As stated at [19]–[21] above, personal mobile numbers are *prima facie* personal data as they are unique identifiers.

Mr Ivan Chua

47 As observed in *Re Sharon Assya Qadriyah Tang*, the purchase of leads, in which the buyer acquired personal data from the seller of the transaction amounts to a “collection” of personal data under the PDPA by the buyer.¹⁶ It is not disputed that Mr Chua collected personal data when he bought the Lists from Amicus and used the personal data to market his team’s financial products. By his own admission, the personal data was collected and used in breach of the Consent and Notification Obligations. Mr Chua also admitted that while he received verbal assurance from Amicus that the information in the datasets was obtained from caveats and was “legal”, he did not probe further as to how, where and when Amicus obtained the personal data, or whether Amicus had obtained consent and provided notification to the individuals concerned.

48 In this regard, reference is made to the UK Information Commissioner’s Office’s (“ICO”) decision in *The Data Supply Company*, where a data broker was found to be in breach of the Data Protection Act 1998¹⁷ for obtaining customer data from various sources and selling the data to third-party organisations for the purposes of direct marketing. The individuals were not informed that their personal data would be 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. The ICO issued a monetary penalty of £20,000 and gave the following guidance in the Monetary Penalty Notice:¹⁸

Data controllers buying marketing lists from third parties must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

Data controllers must take extra care if buying or selling a list that is to be used to send marketing texts, emails or automated calls. The Privacy and Electronic Communications Regulations 2003 specifically require that the recipient of such communications has notified the sender that they consent to receive direct marketing messages from them. Indirect consent (ie consent originally given to another organisation) may be valid if that organisation

16 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [13].

17 c 29.

18 UK Information Commissioner’s Office, “Monetary Penalty Notice: The Data Supply Company Ltd” (27 January 2017) at paras 22–25.

sending the marketing message was specifically named. But more generic consent (eg marketing ‘from selected third parties’) will not demonstrate valid consent to marketing calls, texts or emails.

Data controllers buying in lists must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence. Such due diligence might, for example, include checking the following:

- How and when was consent obtained?
- Who obtained it and in what context?
- What method was used – eg was it opt-in or opt-out?
- Was the information provided clear and intelligible? How was it provided – eg behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Is the seller a member of a professional body or accredited in some way?

Data controllers wanting to sell a marketing list for use in text, email or automated call campaigns must keep clear records showing when and how consent was obtained, by whom, and exactly what the individual was told (including copies of privacy notices), so that it can give proper assurances to buyers. Data controllers must not claim to sell a marketing list with consent for texts, emails or automated calls if it does not have clear records of consent. It is unfair and in breach of the first data protection principle to sell a list without keeping clear records of consent, as it is likely to result in individuals receiving noncompliant marketing.

[emphasis added]

49 While there is no uniform industry standard in relation to how a buyer should verify whether the seller has obtained the consent of the individuals, the positions articulated by the ICO must be right. A reasonable person would likely undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals had provided their consent and were notified of the disclosure, and if so, obtain a sample of such consent and notification.

50 Similarly, organisations that sell datasets should ensure that they obtain and maintain clear records of consent so that proper assurances can be given to buyers.

DIRECTIONS

51 Having found Amicus and Mr Chua to be in breach of ss 13 and 20 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give such directions as he deems fit to ensure compliance with the PDPA.

52 In assessing the breach and determining the directions to be imposed on Amicus, the following aggravating factors were taken into account:

- (a) the personal data disclosed included NRIC numbers which constitute personal data of a sensitive nature;
- (b) Amicus profited from the sale of personal data and admitted that it sold the personal data to others besides Mr Chua;
- (c) Amicus was unhelpful and was not forthcoming in its responses to the Commission during the investigation; and
- (d) Amicus was inconsistent in its responses and kept changing its account of the facts.

53 The following aggravating and mitigating factors were taken into account in assessing the breach and determining the directions to be imposed on Mr Chua:

Aggravating factors

- (a) the personal data was purchased with the intention to market goods and services to individuals for financial gain; and

Mitigating factors

- (b) Mr Chua had co-operated fully with the investigation and played an important and integral role in the investigation. He was forthcoming and admitted to his wrongdoing at the first instance.

54 There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data, which were set out in *Re Sharon Assya Qadriyah Tang*.¹⁹

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

19 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [30].

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. In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data. [emphasis added]

55 The profiting from sale of personal data by organisations without consent of individuals is the kind of activity which the PDPA seeks to curb and will be dealt with severely. In order to prevent abuse by organisations profiting from the sale of personal data at the individual's expense, the Commission may take into account any profits from the unauthorised sale of personal data in calculating the appropriate financial penalty to be imposed.

56 Having considered all the relevant factors of this case, the following directions are made:

To Amicus:

- (a) to pay a financial penalty of \$48,000 (including \$2,900 for the profit made from the sale of Lists 1 and 2) within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court²⁰ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full;
- (b) to cease the disclosure (sale) of the personal data of all the individuals immediately;
- (c) to cease the retention of the said personal data within seven days from the date of the Commissioner's direction, to the extent that such personal data was collected and/or disclosed in breach of the PDPA; and
- (d) to submit a written confirmation to the Commission by no later than one week after each of the above directions in (b) and (c) have been carried out.

To Mr Ivan Chua:

- (e) to pay a financial penalty of \$10,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at

20 Cap 322, R 5, 2014 Rev Ed.

- the rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full;
- (f) to cease the use (telemarketing) of the personal data of all the individuals immediately;
 - (g) to cease the retention of the said personal data within seven days from the date of the Commissioner's direction, to the extent that such personal data was collected in breach of the PDPA; and
 - (h) to submit a written confirmation to the Commission by no later than one week after each of the above directions in (f) and (g) have been carried out.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Marshall Cavendish Education Pte Ltd

[2020] PDP Digest 425

Coram: Tan Kiat How, Commissioner

Case Number: DP-1704-B0699

Decision Citation: [2020] PDP Digest 425; [2019] SGPDPDC 34

Protection Obligation – Unauthorised access to personal data – Insufficient security arrangements

30 August 2019

1 With the increasing prevalence of ransomware attacks online, this case gives occasion to restate the importance of making adequate security arrangements to protect personal data and to limit unnecessary exposure of an organisation’s computer systems to such potential threats on the Internet.

BACKGROUND

2 Marshall Cavendish Education Pte Ltd (“MCE” or “Organisation”) provided a learning management system (“LMS”) at <www.mconline.com.sg> (“Website”) to the Ministry of Education (“MOE”) schools. This was pursuant to a contract between MCE and MOE.

3 On 1 February 2017, ransomware affected a substantial portion of MCE’s network (“Incident”). On 3 February 2017, MCE informed MOE of the Incident. The relevant government agencies were notified of the Incident accordingly, including the Personal Data Protection Commission (“PDPC”). The ransomware had encrypted the files found on MCE’s servers, including files containing personal data of individuals stored in the LMS, and made them inaccessible until a payment was paid to decrypt them.

4 Investigations revealed that the ransomware was an executable file on one server. However, it affected data on 11 servers and network storage devices in MCE’s network. These 11 affected servers and network storage

devices mostly held teaching material. However, the server in question and a network storage device each held copies of the database of 206,240 active and 44,688 inactive users. The database held the following personal data of its users, which were mandatory fields that every user who signed up for accounts on the Website had to provide:

- (a) login ID comprising an individual's full or partial birth certificate or NRIC number;
- (b) name;
- (c) school name;
- (d) schooling level; and
- (e) class.

5 Users could also opt to supply additional personal data using optional fields. According to MCE, however, users rarely provided such additional information, which comprised:

- (a) e-mail address;
- (b) address;
- (c) NRIC number;
- (d) mobile number;
- (e) father/mother/guardian's name;
- (f) father/mother/guardian's NRIC/passport number;
- (g) father/mother/guardian's occupation;
- (h) father/mother/guardian's mobile number;
- (i) father/mother/guardian's residential number; and
- (j) father/mother/guardian's office number.

6 MCE found no evidence that the personal data in its servers had been exfiltrated. MCE's Internet service provider's network logs would have captured the downloading of a database of that size.

7 However, as access had been gained to MCE's servers to upload and execute the ransomware, it meant that the personal data in MCE's servers were exposed to unauthorised access. Further, the encryption of the personal data by the ransomware was an unauthorised modification of the personal data in MCE's servers.

Causes of the Incident

8 The primary cause of the Incident was due to a change made to a firewall rule to allow Internet access to the server. This allowed the external

perpetrator to gain entry into the system to upload and execute the ransomware.

9 MCE had employed a senior system engineer (“SE”) to, amongst other things, maintain MCE’s servers. The SE was part of the Organisation’s IT team that also comprised of another system engineer and a manager (“IT Manager”) who had supervisory duties over the said system engineers. According to the Organisation, the IT Manager, together with the SE and a program manager, was also responsible for managing the services in the Organisation’s datacentre.

10 The SE had found that the backup server’s anti-virus definition was not updating automatically. The SE thought that the anti-virus’ auto-update function was not working properly due to the limited or restricted access to the Internet, and thus the SE changed a firewall rule to allow direct access from the Internet to the server in question (the “Firewall Rule Change”). The Firewall Rule Change had lifted the restrictions that were in place to prevent external access to the MCE backup server and the data it held.

11 Critically, although the Firewall Rule Change was intended to be temporary, the SE had failed to reinstate the firewall rule after completing his investigation, thereby allowing the server to be continuously exposed to Internet access. This increased the risk of an external perpetrator being able to gain entry into the server, as had transpired in this case.

12 PDPC’s investigations revealed that the perpetrator had gained entry to the server through brute force attacks on the server. As a result of these brute force attacks, the perpetrator had uploaded and executed the ransomware on the server on 1 February 2017.

REMEDIAL ACTIONS BY THE ORGANISATION

- 13 The Organisation subsequently took the following remedial measures:
- (a) put in place security arrangements to protect the personal data held in its servers after assessment of their need for remote Internet access;
 - (b) conducted a review of the existing firewall rules in conjunction with an assessment of the remote Internet needs of the IT system;

- (c) engaged an external auditor to conduct a thorough review and audit of MCE's IT system;
- (d) strengthened controls over deployment of any program to the Website;
- (e) strengthened controls over obtaining of source code and database scripts;
- (f) improved handling of any reported defects/issues with the LMS portal;
- (g) implemented monthly review of user access rights, including a listing of product environment users and their accompanying access rights;
- (h) strengthened control of user access requests to the remote desktop protocol ("RDP") server and mechanisms to deal with the deletion of any remote user access requests by non-active accounts;
- (i) improved management of the various types of user accounts;
- (j) better defined scope of duty for each system engineering team;
- (k) hired an IT security officer to focus solely on cybersecurity; and
- (l) strengthened its network security by clarifying various steps or approvals that need to be performed or obtained before a system engineer can make any system changes and procedures for follow-up actions and management reporting for all IT security incidents.

FINDINGS AND BASIS FOR DETERMINATION

Issue for determination

14 The issue to be determined is whether MCE had complied with its Protection Obligation under s 24 of the Personal Data Protection Act 2012¹ ("PDPA") in this case.

15 There is the preliminary issue of whether MCE was a data intermediary for MOE and whether it could avail itself of the exception under s 4(1)(c) of the PDPA, which states that Pts III to VI of the PDPA, including s 24 of the PDPA, shall not impose any obligation on any public

1 Act 26 of 2012.

agency or organisation in the course of acting on behalf of a public agency (in this case, MOE). Investigations disclosed that MCE was a vendor providing IT tools and hosting services for MOE's teaching and administrative programmes. MCE was not acting on behalf of a public agency for the purposes of s 4(1)(c) of the PDPA and is subject to the full gamut of obligations under the PDPA *qua* its capacity as a data intermediary.

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

Whether MCE breached section 24 of the Personal Data Protection Act 2012

17 The personal data in question was stored on MCE's backup server. It was in MCE's possession or under its control. MCE therefore had a duty to protect that data by making reasonable security arrangements against unauthorised access or modification.

18 MCE did not fulfil its obligation under s 24 of the PDPA when the circumstances are viewed in totality. The SE had intended the Firewall Rule Change to be temporary. However, the SE had failed to reverse the Firewall Rule Change as he was interrupted by other work matters in the middle of attempting to establish the reason for the failure of the anti-virus software to update automatically. This was a critical misstep.

19 This was exacerbated by the fact that the SE had, at some time prior to this, already installed remote access software on the backup server. Only the RDP server was meant to be configured to be accessible remotely. However, it appears that the SE had configured the backup server as a secondary RDP server.

20 While the Firewall Rule Change in and of itself was a security risk as it opened the MCE's backup server to a wide range of possible attacks, the installation of remote access software on the server and its configuration as a secondary RDP server would have allowed an attacker a greater chance of success in infiltrating it, especially where no safeguards were implemented to mitigate this risk. These threats are real – as has been exemplified in this

case where the perpetrator had managed to use brute-force attacks to gain access to the backup server in order to upload and execute the ransomware.

21 As an organisation, MCE bore responsibility for putting in place the requisite measures to prevent data breaches from taking place. As mentioned in *Re Aviva Ltd*,² relying solely on employees to perform their tasks diligently is not a sufficiently reasonable security arrangement, and the organisation would need to take proactive steps to protect personal data. In this case, the SE was part of the Organisation's IT team supervised by an IT Manager. However, it appears that the IT Manager did not exercise competent supervision over the IT team. In this regard, the Organisation admitted, through a written statement made by the Organisation's General Manager of Product Development ("GM of Prd Devpt"), that:

- (a) user accounts in the data centre for former staff, including that of a member of staff who had left in 2014, had not at the material time been removed;
- (b) the SE was not familiar with the new firewall and that this may have contributed to the Incident. If the Organisation was aware of the SE's unfamiliarity with the new firewall, the IT Manager ought to have supervised the SE more closely; and
- (c) there were no standard operating procedures in place to document changes to the firewall configurations and there were no measures in place to monitor for the installation of unauthorised software. We have addressed this issue at [35] to [37] below in addressing the representations made by the Organisation.

22 In these circumstances, the IT Manager may not have been able to effectively supervise the daily operational actions of the SE.

23 What is required on the part of the Organisation are practicable steps, and these can take the form of identifying areas of risk that require higher level approval and adequate supervision of such risky areas. One such area that ought to have been identified was the installation of remote access software as every installation of remote access software is a channel for web-based threats that have to be guarded against. In this regard, the Organisation did not implement a process which provided adequate

2 [2019] PDP Digest 145.

supervisory oversight over the installation of the remote access software, apart from identifying the installation of remote access software as an act that required higher-level approval. Records of any installation of the remote access software could also be, but were not, maintained. This would have been a practicable step that MCE could have put in place. Of course, this cannot prevent the situation where the SE wilfully disregarded such a policy and proceeded to install remote access software on the backup server without authority, but the analysis of the facts and conclusion on MCE's liability might well be different had such supervisory measures been implemented.

24 Similarly, MCE could also have implemented some form of approval process for changes to firewall configuration. In this case, a manual record of firewall changes in a log book or other form of supervisory monitoring, for example, could have been practicable steps put in place by MCE. This would have heightened the awareness of the SE that changes to firewall rules cannot be made in a cavalier manner, and that his actions were subject to scrutiny. Again, this will not prevent wilful disregard for such control measures but the lack of such practicable steps deprived MCE room to raise a credible claim that it had put in place reasonable security measures to protect the personal data.

25 In addition to the failure of supervision, 15 accounts with remote access to MCE's system through the primary RDP server were found during MCE's post-Incident review. MCE reduced this number of accounts to five. The unnecessary number of permitted users with remote access to the system pointed to a less than adequate appreciation of the risk that comes with remote access. This buttresses the Commissioner's findings that MCE has not adequately met its s 24 obligation to protect personal data. The personal data stored on the server was not only subject to unauthorised access, it was modified without authorisation through the encryption process of the ransomware.

26 In the premises, the Commissioner is satisfied that MCE failed to make reasonable security arrangements to protect the personal data in its servers from risk of unauthorised access, modification and disposal. The Commissioner therefore finds MCE in breach of its obligation under s 24 of the PDPA.

DIRECTIONS

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

28 Pursuant to s 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that MCE did not make reasonable security arrangements and is in breach of s 24 of the PDPA.

29 Having carefully considered all the relevant factors of this case, the Commissioner hereby directs that MCE pay a financial penalty of \$40,000 within 30 days from the date of the directions, failing which, interest shall be payable on the outstanding amount of such financial penalty.

30 In assessing the breach as determining the directions to be imposed on MCE in this case, the Commissioner took into account the following mitigating factors:

- (a) MCE was co-operative in the investigations;
- (b) there was no misuse of the affected personal data that was reported or indicated; and
- (c) MCE had put in place several remedial measures as indicated at [13] above.

However, the Commissioner had to balance these mitigating factors against the fact that MCE's failure to protect in this case led to loss of personal data in the possession of the organisation to the control of the ransomware attacker.

31 Representations were made by MCE after being informed of the proposed decision in this case, submitting that it had complied with the Protection Obligation under s 24 of the PDPA. In the alternative, MCE requested for a warning in lieu of a financial penalty or to otherwise reduce the quantity of the financial penalty imposed.

Compliance with the Protection Obligation under section 24 of the Personal Data Protection Act 2012

32 In support of the assertion that MCE had complied with s 24 of the PDPA, MCE made the following representations:

- (a) by installing remote access software on the backup server and changing the firewall configuration without higher level approval from MCE's IT manager, the SE *wilfully disregarded* MCE's IT security policy;
- (b) as acknowledged by the Commission at [23] above, no practicable steps can be taken to prevent a situation of wilful disregard; and
- (c) MCE had adequate supervisory measures, as seen by the fact that the Incident was discovered after MCE carried out its routine monitoring of the system, and MCE subsequently took prompt action to investigate the Incident.

33 The Commissioner has considered the representations and maintains his finding that MCE is liable under s 24 of the PDPA for the actions of the SE.

34 At the outset, it is crucial to note that the breach was not one-off, as the SE's installation and usage of the unauthorised remote access software on the backup sever took place on more than one occasion but went undetected. In fact, the SE had fully configured the backup server to function as an RDP server, should the primary server fail, without the knowledge of his supervisor. This shows the inadequacy of MCE's supervisory mechanisms.

35 It should be noted that the Organisation, through a written statement made by its GM of Prd Devpt on 2 June 2017, had admitted that:

- (a) "At the time of the incident, there were no measures in place to prevent system engineers to install unauthorised software, such as Teamviewer [a remote access software]."
- (b) "They [the IT team] were not required to notify anyone else if changes were made to the firewall configurations. There are no standard operating procedures to document such changes." The Organisation also admitted that this was a lapse on its part and has tightened its process following a security audit by its vendor.

36 The Organisation in its representations has stated that it had a policy in place which required the SE to seek higher level approval from the IT Manager for the installation of remote access software and the Firewall Rule Change. Assuming that the statement made by the GM of Prd Devpt on 2 June 2017 and the statements made in the representations are true and are consistent with each other, the reasonable conclusion is that, while there was a policy requiring such higher-level approvals, this policy was not adequately implemented and there was a lack of supervision and monitoring over both the installation of remote access software and the Firewall Rule Change. In practice, the SE was allowed to take whatever action he deemed fit without any supervisory oversight from the IT Manager or any other supervisor even if this resulted in compromising the Organisation's IT security.

37 In this regard, the fact that the SE was able to wilfully disregard MCE's procedures on more than one occasion over a period of time, without this activity being detected, highlighted MCE's failure to translate the policy into a process which sufficiently complies with s 24 of the PDPA. Merely putting in place policies is insufficient to fulfil MCE's obligation under s 24 of the PDPA – MCE must also have taken practicable steps to *implement* these policies, for example, as set out above at [21], through adequate supervision and/or monitoring.

Imposition of financial penalty

38 In support of its request that the Commission should issue a warning instead of a financial penalty or otherwise reduce the quantity of the financial penalty imposed, MCE made the following representations:

- (a) The Commission failed to consider all relevant mitigating factors in arriving at the preliminary decision.
- (b) The proposed financial penalty is manifestly excessive in the light of previous decisions issued by the Commission for similar or even more serious breaches.
- (c) It would be extremely prejudicial for MCE if the Commission were to issue a decision and impose penalties on MCE almost two years after the Incident, as the public may have the misconception that the Incident took place recently and MCE currently does not have reasonable security arrangements to protect personal data that is in its possession.

39 MCE raised the following mitigating factors in its representations:

- (a) there was clearly no loss of personal data;
- (b) no personal data was accessed by the perpetrator or any third party and no individual can or will be affected by the Incident;
- (c) MCE took immediate steps to reduce the damage caused by the Incident;
- (d) there were no prior breaches of the PDPA on the part of MCE; and
- (e) MCE had not acted deliberately or wilfully.

40 As the personal data had been rendered inaccessible by encryption, MCE had in fact lost access and control of the personal data. Also, because of the unauthorised encryption of files containing the personal data, MCE was forced to delete these encrypted files in accordance with its data protection policy. The main database was modified because it was encrypted, and there would have been a loss of new incremental data created during the interval between the last backed-up copy and ransomware attack. Furthermore, personal data was put at risk as the perpetrator of the ransomware attack could access the personal data if they chose to do so.

41 Nevertheless, as noted at [30] above, the Commission took into account the fact that there was no misuse of the affected personal data that was reported or indicated, and the fact that MCE had put in place remedial measures following the Incident. The fact that there were no prior breaches of the PDPA is not a mitigating factor in itself. On the contrary, if MCE had breached the PDPA repeatedly, this would have been an aggravating factor, and it is trite that the absence of an aggravating factor is not a mitigating factor. In addition, the deliberateness or wilfulness of MCE in breaching the PDPA is not a relevant consideration in this case.

42 Furthermore, the three cases cited by MCE – *Re Challenger Technologies Limited*³ (“Challenger”), *Re Institute of Singapore Chartered Accounts*⁴ (“ISCA”) and *Re Bud Cosmetics Pte Ltd*⁵ (“Bud Cosmetics”) are not analogous to the present facts.

3 [2017] PDP Digest 48.

4 [2019] PDP Digest 333.

5 [2019] PDP Digest 351.

43 Firstly, MCE submitted that only a warning was imposed in *Challenger* although the personal data of more than 165,000 individuals was compromised. However, the personal data leaked in *Challenger* was limited – it comprised only individuals’ names, membership expiry dates and accumulated points. However, the personal data in the present case includes personal data of minors and NRIC numbers, and is thus of a more sensitive nature.

44 Secondly, MCE submitted that the personal data compromised in *ISCA* was even more sensitive as it included employment records and examination results; however, a financial penalty of only \$6,000 was imposed. Employment and examination results are not treated as sensitive data. Furthermore, the number of affected individuals in *ISCA* was substantially smaller – 1,906 individuals as opposed to more than 250,000 individuals in the present case, and the unauthorised disclosure was limited to a *single* unintended recipient for a short period of ten minutes. This consequentially affects the quantity of the financial penalty imposed.

45 Thirdly, MCE submitted that in *Bud Cosmetics*, the Commission imposed a financial penalty of only \$11,000 despite the fact that the Commission found breaches under ss 12, 24 and 26 of the PDPA. As with *Challenger*, the personal data compromised in *Bud Cosmetics* was not sensitive. Furthermore, the number of affected individuals in *Bud Cosmetics* was substantially smaller – 2,457 individuals as opposed to more than 250,000 individuals in the present case.

46 Lastly, the time taken to complete investigations into PDPA breaches and issue decisions may vary from case to case due to a myriad of factors. The present case involved substantial technical complexities requiring a longer period of time to complete investigations, consider representations and issue the decision. The present grounds of decision clearly state the date of the Incident and the remedial measures taken by MCE. This would address MCE’s concerns that the public would be of the view that the Incident took place recently or that it has not remediated the breach.

47 In view of the remedial measures taken by MCE, no further directions are necessary.

48 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 organisations will be taken.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Advance Home Tutors

[2020] PDP Digest 438

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1806-B2218

Decision Citation: [2020] PDP Digest 438; [2019] SGPDPDC 35

Accountability Obligation – Lack of data protection policies and practices

Protection Obligation – Unauthorised disclosure of personal data –

Insufficient security arrangements

Protection Obligation – Unauthorised disclosure of personal data – Lack of access controls

15 September 2019

FACTS OF THE CASE

1 On 7 June 2018, the Personal Data Protection Commission (the “Commission”) received a complaint that personal data of many individuals had apparently been disclosed without authorisation on the organisation’s website, <www.advancetutors.com.sg> (the “Website”). Upon investigation, the Commission found the following facts leading to this apparent unauthorised disclosure of personal data.

2 The organisation is a sole proprietor who provides “matching services” through the Website between freelance tutors and prospective clients seeking tuition services (the “Organisation”).

3 In January 2017, the Organisation engaged a freelance web developer based in the Philippines (the “Developer”) to provide the following services:

- (a) to design and develop the Website; and
- (a) to migrate the existing databases and files of the Organisation’s old website to the Website.

4 At that point in time, 834 freelance tutors had signed up with the Organisation and some of these tutors had chosen to upload their

educational certificates to the Website's server (the "Server") via the Website. These certificates would be used by the Organisation to evaluate the suitability of the tutors for prospective jobs. In addition, copies of a tutor's certificates were to be disclosed on the tutor's public profile on the Website if the tutor consented to such disclosure. Out of the tutors who had uploaded educational certificates, a total of 152 tutors (the "Affected Individuals") had not consented to disclosure of their educational certificates on their public profile.

5 The Developer subsequently migrated the educational certificates of the tutors who had uploaded them to the Website and stored them in an image sub-directory of a public directory found on the Server (the "Image Directory"). These directories were not secured with any form of access controls and were accessible by the public via the Internet if the path to the relevant directory was typed into a web browser. Furthermore, no measures were taken to prevent automatic indexing of the Image Directory by Internet search engines. This resulted in the contents of the Image Directory, including the educational certificates of the Affected Individuals, showing up in search results on Google after the Website went live on 17 October 2017.

6 On 6 April 2018, the Organisation informed the Developer to make certain changes to the Website in order to disclose the educational certificates of consenting tutors on their public profile pages on the Website. The Organisation provided written instructions to the Developer to "migrate all existing tutor profiles from the [old website] to the [Website]", and to "impose all pre-existing conditions in the [old website] to the [Website] when migrating the tutors". According to the Organisation, one of the pre-existing conditions of the old website was to only disclose educational certificates of tutors who had consented.

7 The Organisation also represented that it had provided the following verbal instructions to the Developer:

- (a) to "hide the educational certificates of tutors who did not give consent";
- (b) to "respect and protect the privacy and confidentiality of all the data that is present in AHT website";
- (c) it "should not disclose or share any of the personal data or AHT Admin user account details with a third party"; and

- (d) to “ensure users’ data is protected as AHT had entrusted them for the purpose of IT services”.

8 Acting on the Organisation’s instructions, the Developer wrote a coding script to enable the retrieval and display of the educational certificates from the Image Directory. However, the coding script lacked a validation condition to ensure that only educational certificates of tutors who had consented to disclosure were disclosed on the tutors’ profile pages on the Website. This resulted in all of the educational certificates found in the Image Directory, including those of the Affected Individuals, being retrieved and publicly disclosed on the Website through the tutors’ respective profile pages.

9 The disclosure of the Affected Individuals’ educational certificates (described at [5] and [8] above) resulted in the unauthorised disclosure of their personal data which were found on their respective educational certificates (the “Incident”). The disclosed personal data included data such as the individual’s name and NRIC number, educational institutions attended and grades attained for each subject (the “Disclosed Data”).

10 Separately, during the Commission’s investigations, the Organisation admitted that it had not developed or implemented any data protection policies relating to its compliance with the Personal Data Protection Act 2012¹ (the “PDPA”).

REMEDIAL MEASURES TAKEN BY THE ORGANISATION

11 After being notified of the Incident, the Organisation took the following steps to mitigate the effects of the breach and to prevent its reoccurrence:

- (a) deleted all the educational certificates that were stored in the Image Directory;
- (b) ceased retention of any educational certificates received from the tutors;
- (c) requested Google to remove any cached copies of the educational certificates from the Image Directory;

1 Act 26 of 2012.

- (d) conducted a penetration test to discover and address any gaps in its security arrangements in respect of the Website and its server;
- (e) removed all front-end access to the “Search Tutor” and “Tutor Profile” pages of the Website;
- (f) engaged an external system analyst to check the work which may be performed by the Developer in future; and
- (g) developed a data protection policy.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had breached section 24 of the Personal Data Protection Act 2012

12 Although the Organisation had engaged the Developer to provide various services, the Organisation retained possession of and control over the Disclosed Data at all material times. It was responsible for the security arrangements to be implemented on the Website and its backend system, as well as protecting the Disclosed Data.

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

14 To determine whether the Organisation was in breach of s 24, the relevant question is whether it had put in place reasonable security arrangements to safeguard the Disclosed Data hosted on the Website and its Server. As the Disclosed Data included the NRIC numbers of the tutors concerned, it should be borne in mind that NRIC numbers are of special concern as they are “a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual”.² Further, the Commission’s *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers*,³ albeit not effective at the time of the breach, point to the risks and potential impact of any unauthorised use or disclosure of personal data associated with an individual’s NRIC; and the expectation that organisations are to

2 *Re Habitat for Humanity Singapore Ltd* [2019] PDP Digest 200 at [19].

3 Issued 31 August 2018, at para 2.4.

provide a greater level of security to protect NRIC numbers in its possession or control.

15 As the Organisation had engaged the Developer to develop the Website, the onus is on the Organisation to ensure that its security requirements for the Website and Server will be and have been met by the Developer. As part of this, the Organisation could have done the following:⁴

- (a) emphasised the need for personal data protection to the Developer by making it part of the written contract;
- (b) when discussing the Developer's scope of work, required that any changes the Developer made to the Website did not contain vulnerabilities that could expose the personal data, and to discuss whether the Developer had the necessary technical and non-technical processes in place to prevent the personal data from being exposed, accidentally or otherwise; and
- (c) tested the Website before any new changes went live to ensure that the Organisation's instructions to the Developer were properly implemented and that the Website was sufficiently robust and comprehensive to guard against a possible cyberattack.

16 The Organisation admitted to the Commission that "there was a lack of technical expertise within Advance Home Tutor to protect personal data", including the lack of expertise "on how to make the technical assessment and ensure that the assessment is robust enough for adequate protection for personal data". This is also evident from the fact that the Organisation had required the Developer to migrate the information of its then-existing tutors from the old website to the Website "with the exact same conditions imposed" on the old website, without having any idea of how its old website had been configured.

4 Further information on the steps that the Organisation should have taken when outsourcing the development of its Website may be found in Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised 10 July 2018).

17 Similar to *Re Tutor City*⁵ (“*Tutor City*”), the Organisation also did not:

- (a) communicate any specific security requirements to the Developer to protect the personal data stored on the Server;
- (b) make reasonable effort to find out and understand the security measures implemented by the Developer for the Website;
- (c) attempt to verify that the security measures implemented had indeed “respect[ed] and protect[ed] the privacy and confidentiality of all the data that is present on the Website” to the extent expected by the Organisation; and
- (d) conduct any reasonable security testing (*eg*, penetration tests).

18 To be clear, the lack of knowledge on the PDPA or expertise in the area of IT security is not a defence against the failure to take sufficient steps to comply with s 24 of the PDPA. There were resources, including the guides published by the Commission, and skilled personnel available that the Organisation could have relied on to increase its knowledge in the relevant areas or to assist it in complying with its obligations under the PDPA.

19 Related to the above, I note that the Organisation’s purported instruction to the Developer to “respect and protect the privacy and confidentiality of all the data that is present on the Website” does not constitute a security measure. The Organisation should have reviewed the security standard implemented on the Website and provided its Developer with the intended use cases and identified foreseeable risks.⁶

20 More generally, although the Organisation asserted that it had provided verbal instructions to the Developer (see [7] above), these have not been substantiated by any evidence. According to the document entitled “Project Scope” entered into between the Organisation and the Developer, there was no specification relating to the security arrangements that the Developer was required to design into the Website and its backend system. The Organisation ought to have entered into a written agreement with the Developer that clearly stated the standard of compliance that the

5 [2020] PDP Digest 170.

6 *Re Tutor City* [2020] PDP Digest 170 at [18].

Organisation expected its Website and Server to have with the PDPA, and the Developer's responsibilities in this regard.

21 As regards security testing, while the Organisation had conducted some testing of the Website from the functionality perspective, *ie*, to verify that certificates of consenting tutors were disclosed on their profile pages, it did not check the profile pages of non-consenting tutors to ensure their certificates were not disclosed. It also did not check if the Website contained any other vulnerabilities that posed a risk to the personal data hosted on the Server. Had the Organisation done a proper security test, the lack of access controls for the certificates hosted on the Image Directory and the unauthorised disclosure of the certificates of non-consenting tutors on their profiles would have been apparent. It would then have been able to take the necessary steps to rectify these security issues. That said, I understand that the Organisation has, since the Incident, procured the Developer to conduct a penetration test and resolve the high-risk issues identified by it.

22 As regards the lack of access controls, it has been observed in *Tutor City* that technical measures are available that prevent indexing of images by web crawlers, *viz*:⁷

- (a) First, the Organisation could have placed these documents in a folder of a non-public folder or directory.
- (b) Second, the Organisation could have placed these documents in a folder of a non-public folder or directory, with access to these documents being through web applications on the server.
- (c) Third, the Organisation could have placed these documents in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (*eg*, implement a password requirement or an IP address restriction).

23 In view of the above, I find the Organisation in breach of s 24 of the PDPA.

7 *Re Tutor City* [2020] PDP Digest 170 at [21]–[23].

Role of the Developer

24 The Developer's role in data migration constitutes "processing" within the meaning of the PDPA. One of the causes for the breach of the Protection Obligation may be traced to the migration of educational certificates to the Image Directory which was publicly accessible and could be indexed by search engines: see discussion at [4] above. As the Developer is in, and supplied the services from, the Philippines, I intend to refer this aspect of the case to the Philippines National Privacy Commission.

Whether the Organisation had breached section 12 of the Personal Data Protection Act 2012

25 Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Although the Organisation is a sole proprietorship with no employees, it collects a significant amount of personal data from the tutors and clients seeking tuition services via the Website. As such, it is required to have an external data protection policy which sets out its practices relating to such personal data and the purposes for which the tutors' and students' personal data are collected, used and disclosed by the Organisation.

26 In view of the Organisation's admission that it had not developed and implemented any such policies, I also find the Organisation in breach of s 12 of the PDPA.

REPRESENTATIONS BY THE ORGANISATION

27 In the course of settling this decision, the Organisation made representations to waive the imposition of financial penalty for the following reasons:

- (a) The Organisation is a small home business which does not generate much revenue. If the proposed financial penalty is imposed, the Organisation would take five to six years to recover the financial penalty amount based on its annual revenue.
- (b) As a sole proprietor, the Organisation's director neglected operational duties of the business in order to assist the Commission with the investigations into the Incident. This

resulted in a significant drop in the Organisation's annual revenue in 2018 and its revenue has yet to recover.

- (c) The Organisation incurred significant costs in undertaking remedial and preventive actions following the Incident.
- (d) This is the first time a data breach involving the Organisation has occurred.
- (e) The Organisation compared the present case to *Tutor City* ([17] *supra*) with similar facts where only a warning had been issued taking into account the number of affected individuals, the type of and duration for which personal data was at risk, and the remedial actions taken.

28 While accepting full responsibility of its breach of s 12, the Organisation also asserted in its representations that based on the grounds of decision of *Tutor City*, it “implicitly understood that [*Tutor City*] also had no policies and practices meeting the PDPA obligations set in place. However, they were not found in breach of the Section 12”.

29 With respect to the Organisation's representations comparing the present case to *Tutor City*, I would like to emphasise that my decision is based on the unique facts of each case. While the facts may appear similar in two cases, my decision in each case takes into consideration the specific facts of the case and the totality of the circumstances so as to ensure that the decision and direction(s) are fair and appropriate for that particular organisation. In this regard, I would highlight that s 12 of the PDPA was never an issue of concern in *Tutor City* as the organisation in question did, in fact, have the requisite policies and processes. Accordingly, this is not a point that would need to be reflected in *Tutor City*. Unlike *Tutor City*, I have decided that a financial penalty is warranted in this case because the Organisation has been found in breach of ss 12 and 24 of the PDPA, and there was a larger number of individuals' personal data at risk in the present case. I have also taken into consideration the fact that the duration for which personal data was at risk in the present case is significantly shorter than *Tutor City*.

30 Having carefully considered the representations, I have decided to reduce the financial penalty to \$1,000. The quantum of financial penalty has been calibrated after due consideration of the Organisation's financial circumstances and to avoid imposing a crushing burden on the Organisation. Although a lower financial penalty has been imposed in this

case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

OUTCOME

31 In assessing the breaches and determining the directions to be imposed on the Organisation in this case, I also took into account the following mitigating factors:

- (a) the Organisation fully co-operated with the Commission's investigations; and
- (b) the Organisation took prompt action to mitigate the effects of the breaches and prevent recurrence of similar breaches.

32 In consideration of the relevant facts and circumstances of the present case, I hereby direct the Organisation:

- (a) to put in place a data protection policy to comply with s 12 of the PDPA within 60 days of this direction;
- (b) to inform the Commission within seven days of implementing the above; and
- (c) to pay a financial penalty of \$1,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁸ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

8 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Singapore Telecommunications Limited

[2020] PDP Digest 448

Coram: Tan Kiat How, Commissioner

Case Number: DP-1705-B0781

Decision Citation: [2020] PDP Digest 448; [2019] SGPDPDC 36

Protection Obligation – Unauthorised access to personal data – Insufficient security arrangements

12 September 2019

BACKGROUND

1 This case concerns a design issue in a previous version of Singapore Telecommunications Limited’s (the “Organisation”) “My Singtel” mobile app (the “Mobile App”), which resulted in the unauthorised disclosure of the personal data of the Organisation’s customers. The current version of the Organisation’s Mobile App does not have this design issue as it has been fixed.

2 On 17 May 2017, the Personal Data Protection Commission (the “Commission”) received information from an anonymous informant alleging that there was a vulnerability in the Organisation’s Mobile App, which allowed the informant to access the account details of other customers (the “Data Breach”). Following an investigation into the matter, the Commissioner found the Organisation to be in breach of s 24 of the Personal Data Protection Act 2012¹ (“PDPA”). The Commissioner sets out below his findings and grounds of decision.

1 Act 26 of 2012.

MATERIAL FACTS AND DOCUMENTS

3 The Organisation is a telecommunications company in Singapore. The Mobile App was developed by the Organisation's IT team to enable its customers to track their account information and manage add-on services. Communications between the Mobile App and the Organisation's servers are conducted via application programming interfaces ("API").

4 The Organisation's customers can log in to the Mobile App via the following methods:

- (a) Mobile Station International Subscriber Directory Number ("MSISDN") login: where a customer's mobile phone is connected to the Organisation's mobile data network (3G/4G), the Organisation's servers will verify that the MSISDN and IP address of the mobile phones are correct before granting the customer access to the Mobile App;²
- (b) one-time password ("OTP"): through validation of the OTP sent to customers via SMS and entering it in the Mobile App ("OTP login method"); and
- (c) OnePass: by using their OnePass login and password.

5 Customers that log in to the Mobile App via the MSISDN or OTP login method have access to the following data relating to their own account:

- (a) the mobile number used to access the Mobile App;
- (b) related service plan information (*ie*, data, talktime and SMS usage);
- (c) outstanding bill amount;
- (d) bill payment due date; and
- (e) billing account number.

2 Each Mobile Station International Subscriber Directory Number ("MSISDN") is assigned a unique IP address. When a user logs in to the Mobile App via the MSISDN login method, the backend server will verify the MSISDN assigned to that IP address. Once verified, the login attempt will be deemed to be authenticated and the user will be granted access to the Mobile App.

6 In addition to the data mentioned at [5] above, customers that log in to the Mobile App via the OnePass method also have access to all the service information for all Singtel services registered under that Singtel OnePass ID. In addition, if such customers had opted for electronic billing, they would have access to the following data relating to their own account:

- (a) the customer's name;
- (b) the customer's billing address; and
- (c) all Singtel services and corresponding usage (where applicable) under the same billing account number.

7 The anonymous informant claimed that the API on the server could be manipulated by using specialised tools to gain unauthorised access to the account details of other customers through the following methods:

- (a) The MSISDN is a string of numbers that incorporates within it the customer's mobile phone number. By logging in using a legitimate Singtel account via the MSISDN login method and changing the value in the MSISDN field (*ie*, to another customer's mobile phone number)³ that was sent from the Mobile App's API to the Organisation's servers, the informant was able to retrieve the account details (such as the billing account number and billing cycle) of the other customer.
- (b) Thereafter, by logging in using a legitimate Singtel account via the OnePass method and changing the value in the billing account number and billing cycle fields, the informant was able to obtain the customer's bill, which contains further personal data such as the customer's name, billing address and all Singtel services and corresponding usage (where applicable) under the same billing account number.⁴

3 The subscriber's mobile phone number was used by the Organisation's servers to retrieve the subscriber's account and billing details.

4 As mentioned at [6] above.

8 The informant accessed four billing accounts and extracted the customer's name, billing address, billing account number, mobile phone number as well as customer service plans (including data, talk time and SMS usage). While there was no further evidence of unauthorised access, the personal data of approximately 330,000 of the Organisation's customers who were using the Mobile App at the material time were put at risk of disclosure.

9 Although the Organisation had engaged a third-party security vendor to conduct regular security penetration tests on the Mobile App and backend systems (including the API), the tests had not detected the design issue in the API that led to the Data Breach and the Organisation was unaware of it.

10 During the investigation, the Organisation admitted that the Data Breach was caused by a design issue in the API – the application input⁵ was not validated against the login credential used to access the Mobile App before performing the requested operation (the “Direct Object Reference Vulnerability”). Because all request parameters sent by the Mobile App to the Organisation's server during a valid login session were assumed to be valid, once a user was legitimately authenticated to initiate a valid login session on the device (via the MSISDN, OTP or OnePass login methods), the user would be able to intercept and change the field parameters in the API requests between the Mobile App and the server. Notwithstanding, the Organisation asserted that such an action was “not something that a normal user of the App would attempt” and the attacker must be “technically competent” as the changing of the parameters could only be performed on a workstation.

11 Soon after it was notified of the Data Breach, the Organisation took remedial actions to resolve the Direct Object Reference Vulnerability. The Organisation enhanced the API in order to tightly couple the Mobile App user's identifiers to the authenticated session. In this manner, should the parameters be modified during the same authenticated session such that they do not match the Mobile App user's identifiers (*eg*, the MSISDN field is changed to another number and service information such as data usage of

5 Such as the MSISDN for the MSISDN or OTP login method, and the MSISDN, billing account number and billing payment due date for the OnePass login method.

that other number is requested), the user will see an error message and be logged out.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

12 It is not disputed that the subscriber's name, billing address, billing account number, mobile phone number as well as customer service plans (including data, talk time and SMS usage) are "personal data" as defined in s 2(1) of the PDPA ("Personal Data"). There is also no dispute that the PDPA applies to the Organisation as it falls within the PDPA's definition of "organisation". The key issue to be determined in this case is therefore whether the Organisation had complied with its obligations under s 24 of the PDPA.

Whether the Organisation complied with its obligations under section 24 of the Personal Data Protection Act 2012

13 Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. It is not disputed that the Personal Data was in the Organisation's possession and/or control.

14 Having considered the material facts, the Commissioner finds that even though the Organisation had engaged a third-party security vendor to conduct regular penetration tests on the Mobile App and backend systems (including the API), the Organisation failed to put in place reasonable security arrangements with respect to the said API to protect the Personal Data.

15 First, by the Organisation's own admission, the Data Breach was caused by the Direct Object Reference Vulnerability, which was a design issue in the API. The Organisation failed to take into account the risk of manipulation to the parameters sent from the Mobile App's API to the Organisation's servers when designing the Mobile App. The validation of parameters (whether input or non-input fields), which could have prevented unauthorised access to the Personal Data, was not implemented as part of the API's initial design.

16 The Direct Object Reference Vulnerability is a relatively basic design issue and well-known security risk that a reasonable person would have considered necessary to detect and prevent. It was one of Open Web Application Security Project (“OWASP”) 2013’s top ten most critical web application security risks and OWASP recommended, among other things, the usage of indirect object reference as a prevention method.

17 Furthermore, as highlighted in the Commission’s *Guide on Building Websites for SMEs*,⁶ programmers should be aware of the common website vulnerabilities and adopt the appropriate programming techniques and practices to ensure that personal data cannot be exposed through such vulnerabilities. Although the *Guide on Building Websites for SMEs* sets out key considerations for the process of setting up a website, the same principles are similarly applicable when programming a mobile application. This is because the same issues arise when a server responds to requests from a mobile app as when it responds to requests from a web browser.

6.5 Website Programming

6.5.1 When programming the website, programmers should be aware of the common website vulnerabilities, and adopt the proper programming techniques and practices to avoid them. *Programmers can use the OWASP Top 10 vulnerabilities list as guide* and some common vulnerabilities include:

- Injection (e.g. SQL Injection)
- Cross-site scripting
- Buffer overflows
- *Poor authentication & session management*

6.5.2 *Organisations and any engaged IT vendors should ensure that personal data cannot be exposed, either accidentally or by design, through any such vulnerabilities. The website functions should be thoroughly tested or scanned for vulnerabilities, before the website is launched.*

[emphasis added]

18 By failing to take into account the risk of manipulation to parameters sent from the Mobile App’s API to the Organisation’s servers, the Commissioner finds that the Organisation subjected its customers to the risk of actual and potential unauthorised access of their personal data.

19 At this juncture, the Commissioner would like to deal with the Organisation’s claim that exploiting the Direct Object Reference

6 Revised 10 July 2018, at para 6.5.

Vulnerability was “not something that a normal user of the App would attempt” and that the attacker must be “technically competent” as the changing of the parameters could only be performed on a workstation.

20 While the changing of parameters would require a person to have some knowledge of the tools and methods for doing so, anyone with working knowledge of how a mobile app communicates with the servers through an API could have exploited the Direct Object Reference Vulnerability. The tools and software required to manipulate the parameters are available online.

21 The Organisation was aware that direct object reference vulnerabilities had been discovered in its Mobile App. Despite having received professional advice to take precautions against such vulnerabilities, the Organisation omitted to conduct a full code review on the input and non-input fields and hence failed to discover the Direct Object Reference Vulnerability that was exploited in this case.

22 As mentioned at [9] above, the Organisation had engaged a third-party security vendor to conduct regular security penetration tests on the Mobile App and backend systems.⁷ The Direct Object Reference Vulnerability was not detected prior to the Data Breach but a variation of it was found in the October 2015 penetration test (“2015 Penetration Test Report”) and rectified in November 2015. In the 2015 Penetration Test Report, the security vendor cited three examples of direct object reference vulnerabilities in the API (collectively, the “2015 DOR Vulnerabilities”).

23 During the investigation, the Organisation represented that the 2015 DOR Vulnerabilities were specific to the API accepting *input fields* (ie, parameters keyed in by users at the user interface level), whereas the Direct Object Reference Vulnerability did not validate non-input fields (ie, parameters not keyed in by users such as automatically generated URL at the backend). As the Organisation had only conducted a code review for the 2015 DOR Vulnerabilities on APIs accepting *input fields*, the Direct Object Reference Vulnerability that caused the Data Breach was not discovered at the time. However, contrary to the Organisation’s

7 At the time of the Data Breach, the most recent penetration tests on the Mobile App and backend systems were conducted in October 2015 and January 2017.

representation, a review of the 2015 Penetration Test Report showed that both input and non-input fields were affected by the 2015 DOR Vulnerabilities, and even non-input fields could be manipulated by the Mobile App's call to the API and that this should be remedied.

24 Based on the findings and recommendations in the 2015 Penetration Test Report, the Organisation ought to have been more diligent in performing a thorough assessment of the security posture of the API and the server. The Organisation should have examined all other functions to determine whether they could be exploited by changing the input parameters and implement the relevant fixes, but it had failed to do so.

25 For the reasons above, the Commissioner finds that the Organisation is in breach of s 24 of the PDPA as it failed to make reasonable security arrangements with respect to the said API to protect the personal data in its possession and within its control.

26 The Organisation submitted representations after preliminary grounds of decision were issued and raised four points. First, the Organisation asserted that it was reasonable that any request parameters sent by the Mobile App during a login session were treated as valid without having to re-validate the request parameters during the session, given that the user was required to be legitimately authenticated via one of the three login methods. This does not address the Direct Object Reference Vulnerabilities which could be exploited by a third party. Paragraphs [15] to [25] above deal with this point.

27 Secondly, the Organisation asserted that not all of its 330,000 customers' data was put at risk of disclosure as the informant would have had to use the correct combination of the mobile number of the customer, the customer's billing account number, billing account ID and billing cycle date in order to generate a bill specific to that customer or a correct mobile phone number to generate the relevant subscription information. The Organisation thus asserts that the decision should be narrowed to only the four accounts that were successfully accessed. The manner in which the informant was able to access the records of the said four accounts is set out above at [7(a)] and [7(b)]. While the informant only accessed four accounts, the informant or someone with similar skill set and access to the same resources could potentially have access to the personal data of all 330,000 subscribers who were using the Mobile App during the material time of the Incident. In the circumstances, it is correct that the full size of

the database was one of the factors taken into consideration in assessing the financial penalty quantum.

28 Thirdly, in reference to [19] above, the Organisation asserted that the technical expertise required by someone to exploit the Direct Object Reference Vulnerability was underestimated in this decision. For the avoidance of doubt, it is agreed that some level of technical expertise would have been required for someone to exploit the Direct Object Reference Vulnerability. While this level of technical expertise is not uncommon, what cannot be ignored is that the vulnerability is well known and the requisite knowledge, tools and software to exploit the Direct Object Reference Vulnerability can be acquired online. This increases the likelihood that someone with the wrong motivation could have exploited the vulnerability.

29 Finally, the Organisation also restates that the Direct Object Reference Vulnerability was not detected in the security penetration tests. This is dealt with at [21] above.

30 In the circumstances, the Commissioner decided to maintain his finding that the Organisation was in contravention of s 24 of the PDPA. Nevertheless, the Commissioner has decided to impose a reduced financial penalty quantum as set out at [32] below, given that the exploitation of the vulnerability requires some level of technical expertise.

THE COMMISSIONER'S DIRECTIONS

31 Given 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 issue 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.

32 Having considered all the relevant factors in this case, the Commissioner hereby directs the Organisation to pay a financial penalty of \$25,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court⁸ in respect of judgment debts, shall accrue and be payable on the outstanding amount

8 Cap 322, R 5, 2014 Rev Ed.

of the financial penalty until the financial penalty is paid in full. The Commissioner has not set out any further directions given the remediation measures that the Organisation has already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re Zero1 Pte Ltd and another

[2020] PDP Digest 458

Coram: Tan Kiat How, Commissioner

Case Number: DP-1803-B1866

Decision Citation: [2020] PDP Digest 458; [2019] SGPDPDC 37

*Protection Obligation – Unauthorised disclosure of personal data –
Insufficient security arrangements*

16 September 2019

BACKGROUND

1 Zero1 Pte Ltd (“Zero1”) is a mobile virtual network operator founded in 2017. In order to deliver its SIM cards to its customers, Zero1 contracted XDEL Singapore Pte Ltd (“XDEL”) for courier services. In the course of delivering the SIM cards, XDEL inadvertently disclosed the personal data of Zero1’s customers. Central to this case is the question of whether XDEL and Zero1 (collectively referred to as the “Organisations”) had made reasonable security arrangements to protect the personal data of Zero1’s customers pursuant to their obligations under the Personal Data Protection Act 2012¹ (“PDPA”).

MATERIAL FACTS

2 In March 2018, XDEL was appointed by Zero1 to deliver SIM cards to the latter’s subscribers. Zero1’s subscribers would register for mobile services using Zero1’s website. After their application had been processed, Zero1 would provide to XDEL the subscriber’s information (including the subscriber’s name, NRIC number, delivery address and contact number), the SIM card number and the subscriber’s preferred time of delivery. In the

1 Act 26 of 2012.

event that the customer had authorised another person to receive the SIM card on his or her behalf (an “authorised recipient”), the authorised recipient’s information (name, NRIC number, contact number and delivery address) would additionally be provided to XDEL.

3 Each Zero1 subscriber was provided with a unique URL link which would allow them to access a customised delivery notification webpage through which they could monitor the status of their SIM card delivery (the “notification webpage”). It was through the notification webpages that the information of the subscribers and authorised recipients (the “Personal Data”) was accessed.

4 The first batch of SIM card deliveries took place between 8 and 9 March 2018; 333 URLs linking to notification webpages containing the Personal Data of 292 individuals were sent out in support of this first batch of deliveries. Investigations revealed that there was unauthorised access (“Unauthorised Access”) to 175 of the URLs which contained Personal Data. These URLs were accessed by 82 unique IP addresses over a span of about 34 hours, between 12 and 13 March 2018.

5 The Unauthorised Access was discovered after a post on an online forum thread warned other users not to reveal their Zero1 account numbers in public, indicating that it was possible to access another individual’s delivery notification if one was able to determine another subscriber’s membership number. The membership number of another subscriber was not difficult to determine as the membership numbers were generated in sequential order.

6 Further investigations uncovered the following causes leading to the Unauthorised Access of the Personal Data:

- (a) Each notification webpage URL comprised of what XDEL called an “A code” and a “B code”. A sample notification webpage URL took the following form: “https://www.xdel.com/ib/?A=00000000&B=4CC5”. In this example, the A code is 00000000 and the B code is 4CC5.
- (b) The A code is a Zero1 subscriber’s membership number and also the consignment note value, which, as noted above, is a sequentially generated number.
- (c) The B code is the last four characters of a calculated code, generated using a SHA1 hash on the consignment note number, with a secret salt. The B code served as a confirmation code.

It was meant to secure the URLs against unauthorised access. The webpage was supposed to return the delivery status only when the correct B code of four-character length was presented. The calculated B code of four characters meant that it was unlikely that an individual would be able to guess the correct code based on the A code, as there would have been 65,536 possible combinations.

- (d) According to XDEL, the notification webpage system was developed in-house. In the course of investigations, XDEL admitted that its developer had failed to test for the scenario where a blank B code was presented.
- (e) If B codes containing fewer than four characters were presented, the system would only check that the partial code presented matched the ending characters of the correct code. As such, if someone guessed the A code of a subscriber (which as mentioned above was easy enough to do given that the A code is a sequentially generated subscriber number) and left the B code blank, the system would identify this as a correct code, and unauthorised access would be granted to the subscriber's personal data. By altering the A code values, this allowed individuals to see another person's delivery orders and their personal data.

Accordingly, the Unauthorised Access would likely have been prevented if the system was programmed to check the complete B Code instead of a partial code.

THE COMMISSIONER'S FINDINGS AND BASIS FOR DETERMINATION

The relevant Personal Data Protection Act 2012 provisions

7 In respect of this matter, the relevant provision is s 24 of the PDPA. 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 (the "Protection Obligation").

Preliminary issues

8 It is not disputed that the Personal Data is “personal data” as defined in s 2(1) of the PDPA. There is no question or dispute that the Organisations fall within PDPA’s definition of an “organisation”.

9 It is also not disputed that the Protection Obligation applies to both Zero1 and XDEL:

- (a) The personal data of the Zero1 customers and the authorised recipients originated from Zero1 and was under Zero1’s possession and/or control. For this reason, Zero1 had the obligation under s 24 of the PDPA to protect the personal data of its customers and that of the authorised recipients.
- (b) XDEL was the data intermediary for Zero1. XDEL had entered into the “Service Agreement for the Provision of Domestic Courier Services” on 1 March 2018 (the “service agreement”). Pursuant to the agreement, XDEL was to provide for the storage of SIM cards, packing materials, and delivery service. Clause 11 of the agreement stated that XDEL would “process the Personal Data” strictly for the purposes of providing the stated services to Zero1. This would necessarily encompass the processing of the personal data of Zero1’s subscribers for the purposes of delivery. By virtue of s 4(2) of the PDPA, XDEL had the same obligation under s 24 of the PDPA to protect the personal data of Zero1’s subscribers and that of the authorised recipients.

10 The key issue is therefore whether the Organisations had protected the Personal Data in their possession and under their control by making reasonable security arrangements to prevent unauthorised access and similar risks.

Both Organisations failed to make reasonable security arrangements

11 After a review of all the evidence obtained by the Personal Data Protection Commission (“PDPC”) during its investigation and for the reasons set out below, the Commissioner is of the view that both Organisations had failed to make reasonable security arrangements to protect the personal data in their possession and control, and both have thereby breached the Protection Obligation under s 24 of the PDPA.

Breach of the Protection Obligation by Zero1

12 Zero1 was aware of the use of the notification webpage and had defined the type of information contained on the webpage. Presumably, Zero1 had assessed the necessity and risks of the personal data displayed on the notification webpage. Zero1 ought also to have satisfied itself that XDEL had put in place the reasonable security arrangements indicated in the service agreement, before allowing the webpage to be put into use. Zero1 failed to demonstrate it had done the above. It had relied entirely on the warranty with regard to data protection in the service agreement, as well as customer references provided by XDEL.

13 Reasonable security arrangements in this case would entail minimally making an effort to identify the possible risks and seeking assurance that the data intermediary had taken steps to protect against those risks. Unfortunately, Zero1 failed to do either. In fact, Zero1 was not even aware of the security arrangements undertaken by XDEL; neither did it make any effort to identify potential risks associated with the notification webpage. Zero1 has cited a lack of ability and expertise to audit XDEL's notification webpage source code as a reason for not doing so. This cannot be a valid defence as what is required is not technical oversight but an identification of foreseeable risks, and then requiring XDEL to take reasonable measures to address them. The extent of Zero1's due diligence in the circumstances did not require technical knowledge, but risk identification and assessment. For instance, Zero1 could have identified the risk as whether a stranger coming across the website would be able to make changes to it and retrieve a subscriber's information; similarly, whether all information displayed on the notification page was necessary for the subscriber to monitor his SIM card delivery. Having articulated the risks, Zero1 ought to have worked with XDEL on assessing the likelihood of their occurrence, impact on subscribers should the risk occur and what steps XDEL could propose that would be reasonably effective in preventing the occurrence of the identified risks and, should they nevertheless occur, minimise the impact of the risks. This process does not require technical expertise on the part of Zero1; and allows it to rely on XDEL to provide the technical expertise during the risk assessment and mitigation discussion.

14 It is therefore assessed that Zero1 did not meet the standard of having reasonable security arrangements in place.

Representations submitted by Zero1

15 Zero1 submitted its representations to the PDPC after a preliminary decision was issued:

- (a) Zero1 had taken measures to identify and mitigate potential risks. As Zero1 did not have technical capabilities in coding, cybersecurity or data encryption, it relied on XDEL's declarations and assurances of its capabilities and track record. Zero1 also visited XDEL's operation centre to audit its processes and was satisfied that there were no foreseeable risks.
- (b) It is unreasonable to expect Zero1 to pinpoint the possible avenues by which personal data could be compromised. The Incident could not have been pre-empted by Zero1 without the relevant experience and technical knowledge.

16 Zero1 had previously highlighted that it lacks technical expertise and this has already been dealt with at [13] above. It should be pointed out that while Zero1 may have audited the operation centre, this does not detract from the matters raised at [12] above.

17 In relation to the second point raised in [15(b)] above, what was required is for Zero1 to have engaged XDEL on the security arrangements that it had put in place to protect the personal data on the notification webpage, including generating URLs using the membership number and the B Code. This did not require technical expertise on the part of Zero1. It is in the failure to do so that the present breach is found.

18 In the circumstances, the Commissioner maintained his finding that Zero1 is in breach of s 24 of the PDPA.

Breach of the Protection Obligation by XDEL

19 XDEL created the notification webpage system knowing that it would be used to contain the personal data of Zero1 subscribers and their designated authorised recipients.

20 XDEL ought to have taken reasonable security arrangements to protect the personal data from unauthorised access. The reasonable arrangements in this case include adequate testing to verify that the measures were correctly implemented. In this regard, XDEL had implemented the B code to prevent unauthorised access of the notification

webpage. The B code would have prevented unauthorised access had it worked as intended.

21 However, while XDEL tested the notification webpages to make sure they could not be accessed by an incorrect B code, it failed to test for scenarios where the B code was absent or when an incomplete B code was used. Since the B code was, by design, a four-character field, it would seem obvious that the module should have been designed to cater for the situation where the B code did not meet this condition and thereafter to test for this scenario. Given that the B code was crucial to the verification of the user and granting the user access to the user's personal data, tests should have been conducted to ascertain the behaviour of the webpage in the absence of the B code. Its failure to do such tests rendered its efforts to reasonably secure the Personal Data hosted on the notification webpage insufficient.

22 Accordingly, it is assessed that XDEL, like Zero1, did not meet the standard of having reasonable security arrangements in place. XDEL's failure to meet this standard is more serious than that of Zero1, given that XDEL was the party that was responsible for the webpage notification system that failed.

Representations by XDEL

23 XDEL submitted representations to the PDPC on the quantum of the financial penalty only. It asked for a reduction of the financial penalty quantum as it had recently incurred expenses to relocate to new premises. As this is not a mitigating factor or relevant in determining the financial penalty quantum, the Commissioner has decided to maintain the initial financial penalty quantum. Given its current cash flow considerations, the Commissioner has varied his directions to XDEL, as set out below, to allow XDEL to pay the financial penalty in instalments.

THE COMMISSIONER'S DIRECTIONS

24 Having found the Organisations to be in breach of s 24 of the PDPA, the Commissioner is empowered under s 29 of the PDPA to give the Organisations such directions as he deems fit to ensure compliance with the PDPA.

25 In determining the appropriate directions to be imposed on each of the Organisations, the Commissioner has taken into account the following aggravating factors:

- (a) The Personal Data disclosed, which included the personal addresses of the subscribers and authorised recipients, as well as their NRIC numbers, was sensitive in nature.
- (b) Approximately 292 individuals were affected by the unauthorised access.

26 The following mitigating factors have also been taken into account:

- (a) Zero1 voluntarily notified the PDPC that the Personal Data of the subscribers and authorised individuals had been breached.
- (b) XDEL acted swiftly to rectify the notification webpage system. By 13 March 2018, it had managed to modify the code checking function on the webpage to check for the length of the confirmation code, thereby correcting the technical vulnerability. XDEL also added an “alert trigger” that would notify its IT department if an IP address entered three or more consecutive wrong codes, as an additional control to prevent any further unauthorised access.

27 Having considered all the relevant factors of the case, including the relative responsibilities and culpabilities of both organisations, the Commissioner hereby makes the following directions:

- (a) Zero1 is to pay a financial penalty of \$4,000 within 30 days from the date of the Commissioner’s direction, failing which, interest, at the rate specified in the Rules of Court² in respect of judgment debts, shall accrue and be payable on the outstanding amount until the financial penalty is paid in full; and
- (b) XDEL is to pay a financial penalty of \$7,000 in three instalments as set out below, failing which, the full outstanding amount shall become due and payable immediately and interest, at the rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full:

2 Cap 322, R 5, 2014 Rev Ed.

- (i) first instalment of \$2,500 within 30 days from the date of the Commissioner's direction;
- (ii) second instalment of \$2,500 within 60 days from the date of the Commissioner's direction; and
- (iii) third instalment of \$2,000 within 90 days from the date of the Commissioner's direction.

28 Given the remediation efforts undertaken by the Organisations, no further directions relating to the breach itself are issued.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re EU Holidays Pte Ltd

[2020] PDP Digest 467

Coram: Tan Kiat How, Commissioner

Case Number: DP-1901-B3254

Decision Citation: [2020] PDP Digest 467; [2019] SGPDPDC 38

Accountability Obligation – Lack of data protection policies and practices

Protection Obligation – Unauthorised disclosure of personal data

4 October 2019

INTRODUCTION

1 On 14 January 2019, the Personal Data Protection Commission (the “Commission”) received a complaint that personal data of EU Holidays Pte Ltd’s (the “Organisation”) customers was accessible through its website (the “Incident”).

FACTS OF THE CASE

2 Pursuant to a quotation of services dated 16 May 2017 (“Contract”), the Organisation engaged an IT vendor (the “Vendor”) to develop a new website with e-commerce capabilities (the “Website”). One of the purposes of the Website was to allow the Organisation’s customers (“Customers”) to make online reservations for tour packages either directly or through the Organisation’s partner agents. Information relating to travel reservations received from Customers was stored in two web directories. For reservations made directly by Customers on the Website, the tax invoice generated would be stored in a web directory (“Web Directory 1”). As for reservations made through the Organisation’s partner agents on the Website, the tax invoice generated would be stored in another web directory (“Web Directory 2”).

3 The scope of work in the Contract did not specify any requirements with respect to the storage and protection of Customers' personal data which was collected through the Website. The Website was launched on 9 December 2017. Since its launch, the Organisation has been managing the Website, with the Vendor's role limited to maintenance and technical troubleshooting.

4 On or around 5 January 2019, a member of the public ("Complainant") discovered copies of tax invoices containing Customers' personal information while browsing for tour packages on the Website. The Complainant notified the Commission of the Incident on 14 January 2019.

5 Based on the Organisation's internal records, from 9 December 2017 to 14 January 2019, tax invoices containing information of 1,077 Customers were exposed to unauthorised access and disclosure through links to Web Directory 1 and Web Directory 2.¹ The information contained in the invoices includes the following personal data (collectively, the "Disclosed Personal Data"):

- (a) name;
- (b) e-mail address;
- (c) address;
- (d) contact number;
- (e) booking date;
- (f) travel destination;
- (g) departure date;
- (h) gender;
- (i) date of birth;
- (j) passport details (including number, date of issue and expiry);
- (k) rooming arrangement (*ie*, whether travellers are adults or children and the type of beds required); and
- (l) amount payable.

6 Upon being notified of the Incident, the Organisation promptly carried out the following remedial actions:

- (a) deleted all tax invoices stored on Web Directory 1; and
- (b) disabled public access to Web Directory 2.

1 Specifically, the information of 336 Customers was stored in Directory 1 and the information of 741 Customers was stored in Directory 2.

7 Separately, the Commission's investigations revealed that the Organisation had not developed or implemented any internal data protection policies that are necessary for it to meet its obligations under the Personal Data Protection Act 2012² (the "PDPA").

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had contravened section 24 of the Personal Data Protection Act 2012

8 As a preliminary point, the Organisation owned and managed the Website and had possession and control over the Disclosed Personal Data at all material times. While the Vendor had been engaged to develop the Website and subsequently provided maintenance and technical troubleshooting services, the Vendor had not processed the Disclosed Personal Data on the Organisation's behalf. The Vendor was therefore not a data intermediary of the Organisation, and the Organisation was solely responsible for the protection of the Disclosed Personal Data under the PDPA.

9 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. In the Commissioner's view, the Organisation failed to put in place reasonable security arrangements to protect the Disclosed Personal Data as explained below.

10 First, the Organisation failed to assess the risks to the Disclosed Personal Data collected through its Website and stored in Web Directory 1 and Web Directory 2. The investigations revealed that the Organisation had left it to the Vendor to put in place the appropriate security arrangements to protect the Disclosed Personal Data. Consequently, as mentioned at [3] above, the scope of work in the Contract did not include any requirements with respect to how the Disclosed Personal Data was to be stored or protected. The Organisation also did not review the standard of security of the Website and left it completely to the Vendor. In particular:

2 Act 26 of 2012.

- (a) In relation to Web Directory 1, prior to the Incident, since the Organisation did not provide any instructions to the Vendor on the storage of tax invoices generated from direct reservations on its Website, it was unaware that such tax invoices were stored in Web Directory 1 which was publicly accessible. In this regard, the Organisation's assertion was that it had intended for these tax invoices to be stored in a backend content management system which only authorised staff could log into and access. Its intention was not translated into action.
- (b) In relation to Web Directory 2, the Organisation intended for tax invoices generated from reservations through its partner agents to be stored in Web Directory 2 and accessed by partner agents using their respective e-mail addresses and passwords. The Organisation asserted that it did not intend for Web Directory 2 to be publicly accessible. However, since the Organisation did not provide any instructions to the Vendor in relation to access controls for Web Directory 2, none was implemented.

11 What is expected from organisations contracting professional services to build their corporate websites or other online portals is explained in the Commission's *Guide on Building Websites for SMEs*.³ In particular, organisations that engage IT vendors to develop and/or maintain their websites should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms.⁴ Given that the development of the Website was for the purposes of e-commerce (including the collection of Customers' Disclosed Personal Data in relation to reservations for tour packages), the Organisation's failure to specify clear requirements with respect to the protection of personal data is particularly glaring in this case.

12 Secondly, and as observed in *Re Tutor City*,⁵ where documents containing personal data have to reside in web servers, folder or directory permissions are common and direct methods of controlling access and

3 Revised 10 July 2018.

4 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised 10 July 2018) at para 4.2.1.

5 [2020] PDP Digest 170 at [21]–[23].

preventing unauthorised access by public users and web crawlers. Depending on its business needs and circumstances, the Organisation could have instructed the Vendor to implement any of the following reasonable technical security measures to protect the Disclosed Personal Data:

- (a) Place documents containing the Disclosed Personal Data in a non-public folder/directory.
- (b) Place documents containing the Disclosed Personal Data in a non-public folder or directory, with access to these documents controlled through web applications on the server.
- (c) Place documents containing the Disclosed Personal Data in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (*eg*, implement a password requirement or an IP address restriction).

13 In view of the above, the Commissioner found that the Organisation had contravened s 24 of the PDPA.

Whether the Organisation had contravened section 12 of the Personal Data Protection Act 2012

14 Section 12 of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and communicate information about such policies to its staff.

15 By the nature of its business as a travel agency, the Organisation regularly collects personal data of customers to fulfil reservations for tour packages. Notwithstanding this, the Organisation did not have any internal data protection policies to provide guidance to its employees on the handling of such personal data.

16 In the circumstances, the Commissioner found that the Organisation had contravened s 12 of the PDPA.

THE COMMISSIONER'S DIRECTIONS

17 In determining the directions, if any, to be imposed on the Organisation under s 29 of the PDPA, the Commissioner took into account the following mitigating factors:

- (a) the Organisation took prompt remedial actions following the Incident;
- (b) the Organisation was co-operative during the investigations; and
- (c) although the Disclosed Personal Data of 1,077 Customers was at risk of unauthorised access and disclosure, actual disclosure was only to the Complainant in respect of Customers' Disclosed Personal Data in 20 invoices albeit for a period of more than one year.

18 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to:

- (a) Pay a financial penalty of \$15,000 within 30 days from the date of the directions, failing which, interest, at the rate specified in the Rules of Court⁶ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.
- (b) Complete the following within 60 days from the date of this direction:
 - (i) review the security of the Website and implement appropriate security arrangements to protect personal data in its possession and/or under its control;
 - (ii) put in place a data protection policy, including written internal policies, to comply with the provisions of the PDPA; and
 - (iii) develop a training programme for the Organisation's employees in respect of their obligations under the PDPA when handling personal data and require all employees to attend such training

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

6 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Ninja Logistics Pte Ltd

[2020] PDP Digest 473

Coram: Tan Kiat How, Commissioner

Case Number: DP-1804-B2020

Decision Citation: [2020] PDP Digest 473; [2019] SGPDPDC 39

Protection Obligation – Unauthorised access to personal data – Insufficient security arrangements

14 October 2019

INTRODUCTION

1 Ninja Logistics Pte Ltd (the “Organisation”) is a logistics company providing packaging, delivery and tracking services on behalf of retailers (“Retailers”) to the Retailers’ customers (“Customers”). This case concerns the disclosure of personal data via a delivery order tracking function on the Organisation’s website (the “Tracking Function Page”).

2 On 23 April 2018, the Personal Data Protection Commission (the “Commission”) received a complaint that the Tracking Function Page could potentially be used to harvest personal data of the Customers. By changing a few digits of a “Tracking ID”, the complainant could access personal data of another Customer (the “Incident”).

FACTS OF THE CASE

3 The Organisation first set up the Tracking Function Page in December 2014 to allow Customers to (a) inquire about the delivery status of their parcels; and (b) confirm the identity of individuals who collect parcels on their behalf (where applicable). Generally, for a delivery, only a Retailer and the relevant Customers of the Retailer would be provided with a Tracking ID for parcels sent by the Retailer that were to be delivered by the Organisation to the Customer.

4 There were two types of Tracking IDs used by the Organisation, namely sequential and non-sequential Tracking IDs. According to the Organisation, the reason for having sequential numbers in some of the Tracking IDs was for recording and business analytics purposes. Since the launch of the Tracking Function Page, the Organisation was aware that Tracking IDs could potentially be manipulated by changing the last few digits of the Tracking ID. While Tracking IDs with non-sequential numbers may have a lower risk of manipulation, a random generation of any nine digits that happened to match a valid Tracking ID could still result in unauthorised access and disclosure of personal data.

5 For a period of approximately three months from the launch of the Tracking Function Page, the Organisation unsuccessfully experimented with two methods as a second layer of authentication to the Tracking IDs. These methods involved using either the last four digits of a Customer's mobile number or the Customer's last name to verify the identity of the person using a Tracking ID. According to the Organisation, these methods were not workable due to difficulties such as the Retailers not having, or not wishing to disclose, the mobile number of their Customers or the Customers not being able to recall the name they had provided at the time of purchase. Hence, the Organisation ceased using a second layer of authentication in 2015.

6 At the material time, the Tracking IDs were thus the sole means of using the Tracking Function Page. Upon the entry of a valid Tracking ID, the following types of information (the "Disclosed Data") could be accessed from the Tracking Function Page, depending on the delivery status of the parcel in question (as indicated below):

- (a) for parcels with a "Pending Pickup" status:
 - (i) only the Tracking ID;
- (b) for parcels with a "On Vehicle for Delivery" status:
 - (i) the Tracking ID; and
 - (ii) the Customer's Address; and
- (c) for parcels with a "Completed" status:
 - (i) the Tracking ID;
 - (ii) the Customer's address; and
 - (iii) the name and signature of the Customer or other individual who had collected the parcel on behalf of the

Customer (this was upon clicking on the “Retrieve Proof of Delivery” hyperlink).

7 Save for the one-time archival of 2.6m Tracking IDs on 31 August 2016, the Organisation did not have any procedures to remove records of completed deliveries from the Tracking Function Page (*ie*, those with the “Completed” status). The Organisation estimated that, at the time of the Incident, there were 1,262,861 unique individuals with valid Tracking IDs at the “Completed” status (the “Affected Individuals”).

8 Upon being notified by the Commission of the Incident, the Organisation took the following remedial actions:

- (a) removed the Customer’s address for the “Pending Pickup” and “On Vehicle for Delivery” delivery statuses;
- (b) as of 23 August 2018, the Organisation implemented a system such that Tracking IDs would expire 14 days after the completion of the delivery;¹
- (c) in August 2018, the Organisation engaged a Crest-certified security organisation for a one-year period to assist with establishing an overarching security framework with a data protection focus, which includes working out a data protection training programme for the Organisation’s employees who will all receive formal training on the Organisation’s obligations with respect to the Personal Data Protection Act 2012² (“PDPA”); and
- (d) engaged a law firm to improve and document the Organisation’s personal data protection policies.

FINDINGS AND BASIS FOR DETERMINATION

9 As a preliminary point, the Disclosed Data for parcels with “Pending Pickup” and “On Vehicle for Delivery” delivery statuses did not include any data that could identify a Customer. However, the Disclosed Data for

1 The Organisation has since received feedback from some Retailers requesting to lengthen the validity period of the Tracking IDs, and is considering lengthening the validity period from 14 days to 45 days, but this has yet to be implemented.

2 Act 26 of 2012.

parcels with the “Completed” delivery status included the Customer’s name, address and signature. Hence, such data constituted personal data where it related to an identified Customer. In particular, the Incident resulted in the exposure of the following personal data to unauthorised access (the “Exposed Personal Data”):

- (a) the names and signatures of Affected Individuals who had signed for parcels when collecting them; and
- (b) potentially, the addresses of Affected Individuals who were Customers.

Whether the Organisation had contravened section 24 of the Personal Data Protection Act 2012

10 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Commissioner found that the Organisation had failed to put in place reasonable security arrangements to protect the Exposed Personal Data for the following reasons:

- (a) First, and as mentioned at [4] above, the Organisation was aware from the outset that Tracking IDs may be manipulated and had tried unsuccessfully to introduce a second layer of authentication. Notwithstanding its knowledge of the risk of unauthorised access and disclosure of the Exposed Personal Data through manipulation of the Tracking IDs, there was a glaring failure by the Organisation to operationalise an effective method of second layer authentication. Given the foreseeable risk of using Tracking IDs as the sole means of accessing and using the Tracking Function Page, it is inexcusable for the Organisation to neglect its obligations to implement a workable security arrangement to protect the Exposed Personal Data. This resulted in the Exposed Personal Data of a significantly large number of individuals being exposed to the risk of unauthorised access and disclosure for a period of close to two years.
- (b) Secondly, the Organisation did not have a procedure to remove the Exposed Personal Data from the Tracking Function Page after the completion of a delivery. The Organisation could have

easily done so by setting a fixed period upon completion of a delivery after which the Tracking ID would no longer be valid (as it has done after being informed of the Incident). This would have significantly reduced the risk of unauthorised access and disclosure to the Exposed Personal Data.

11 Accordingly, the Commissioner found that the Organisation had contravened s 24 of the PDPA.

REPRESENTATIONS BY THE ORGANISATION

12 In the course of settling this decision, the Organisation made representations for the Commissioner to issue a warning in lieu of a financial penalty, or in the alternative, to reduce the quantum of financial penalty imposed for the reasons set out below.

13 First, on 31 August 2016, the Organisation archived a significant number (2.3 m) of Tracking IDs. As such, only Tracking IDs issued after 31 August 2016 were accessible at the date of the Incident (*ie*, the Exposed Personal Data was subject to risk of unauthorised access and disclosure for less than two years).³

14 Secondly, keeping the Exposed Personal Data accessible from the Tracking Function Page was “well-meaning and intended to be an additional feature of its platform to differentiate itself from its competitors”, and this allowed the Retailers and their Customers to access such information as and when required without having to contact the Organisation. Furthermore, some Retailers may not receive feedback from its customers promptly and would require the Tracking IDs to be accessible for a longer period in order to respond to feedback or conduct investigations.

15 Thirdly, the Organisation raised the following factors for the Commissioner’s consideration:

3 Prior to the Organisation providing information in relation to the archiving of Tracking IDs on 31 August 2016, the Commissioner preliminarily found that the Exposed Personal Data was subjected to the risk of unauthorised access and disclosure for more than two years.

- (a) the names in the Exposed Personal Data may not be the full names of the Affected Individuals and are “considerably less sensitive and complete than other published cases”;
- (b) there was only a single finding of breach of one obligation under the PDPA (*ie*, s 24); and
- (c) there was no evidence to suggest any actual unauthorised access and/or exfiltration of data leading to loss or damage.

16 Finally, the Organisation also compared the present case with *Re K Box Entertainment Group Pte Ltd*⁴ (“*K Box*”) and *Re Horizon Fast Ferry Pte Ltd*⁵ (“*Horizon Fast Ferry*”). The Organisation represented that the circumstances of these two cases were far more aggravated in comparison and the financial penalties imposed were \$50,000 in *K Box* and \$54,000 in *Horizon Fast Ferry*. The Organisation also represented that *Re Challenger Technologies Limited*⁶ (“*Challenger*”) is more similar to the present case, and a financial penalty was not imposed in *Challenger*.

17 Having carefully considered the representations, the Commissioner has decided to maintain the quantum of financial penalty set out at [20(a)] below for the following reasons:

- (a) While the Organisation did archive 2.6m Tracking IDs on 31 August 2016, this was a one-off exercise. The Organisation did not have any procedures to remove records of completed deliveries from the Tracking Function Page (*ie*, those with the “Completed” status). Notwithstanding the archival of the 2.6m Tracking IDs, Exposed Personal Data of 1,262,861 unique individuals with Tracking IDs had been accumulated over a period of close to two years. This was not reasonable considering that the delivery information which Retailers and Customers may want to access would be for a limited post-delivery period (which was likely to be in the order of weeks rather than years).
- (b) As for the factors in [15] above raised by the Organisation, these had already been taken into consideration in the Commissioner’s determination of the quantum of financial penalty.

4 [2017] PDP Digest 1.

5 [2020] PDP Digest 357.

6 [2017] PDP Digest 48.

- (c) With respect to the Organisation's representations comparing the present case to *K Box*, *Horizon Fast Ferry* and *Challenger*, the key distinguishing factor is the volume of personal data involved. The present case involves over one million Affected Individuals, which far exceeds the number of affected individuals in *K Box*, *Horizon Fast Ferry* and *Challenger*.⁷ These cases therefore do not support the Organisation's representations for a warning to be issued in lieu of a financial penalty or a reduction in financial penalty.

THE COMMISSIONER'S DIRECTIONS

18 In determining the directions to be imposed on the Organisation under s 29 of the PDPA, the Commissioner took into account the following aggravating factors:

- (a) the Organisation was cognisant of the risks of unauthorised access and disclosure to the Exposed Personal Data through the Tracking Function Page but failed to resolve the issue for more than two years;
- (b) the Exposed Personal Data of a significantly large number of individuals were exposed to the risk of unauthorised access and disclosure for close to two years; and
- (c) the Organisation failed to remove Exposed Personal Data of a significantly large number of individuals from the Tracking Function Page when it was no longer necessary to keep them accessible online.

19 The Commissioner also took into account the following mitigating factors:

- (a) the Organisation was co-operative in the investigations;
- (b) the Organisation had, in effect, adopted an approach consistent with data protection by design by controlling the amount of

7 As compared to 1,262,861 unique individuals in this case, the number of affected individuals was found to be approximately 317,000 in *Re K Box Entertainment Group* [2017] PDP Digest 1, 295,151 in *Re Horizon Fast Ferry* [2020] PDP Digest 357 and 165,306 in *Re Challenger Technologies Limited* [2017] PDP Digest 48.

information disclosed at different stages of the delivery process, thereby decreasing the risk of unauthorised access and disclosure; and

- (c) there was no evidence of exfiltration of the Exposed Personal Data.

20 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to:

- (a) pay a financial penalty of \$90,000 within 30 days from the date of the directions, failing which, interest, at the rate specified in the Rules of Court⁸ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full; and
- (b) within 30 days from the date of this direction, implement a reasonable validity period for the Tracking IDs after completion of each delivery, which should be as reasonably short as possible while meeting business needs.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

8 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re SearchAsia Consulting Pte Ltd

[2020] PDP Digest 481

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1809-B2790

Decision Citation: [2020] PDP Digest 481; [2019] SGPDPDC 40

Protection Obligation – Unauthorised access to personal data – Insufficient security arrangements

24 October 2019

INTRODUCTION AND MATERIAL FACTS

1 SearchAsia Consulting Pte Ltd (the “Organisation”) is a recruitment company established in Singapore which matches job seekers with organisations that are looking to recruit employees for a specific role. On 26 September 2018, the Organisation notified the Personal Data Protection Commission (the “Commission”) of a data breach incident involving the inadvertent disclosure of résumés (the “Incident”) which were uploaded by individual job seekers to the Organisation’s website, <www.searchasia.com.sg> (the “Website”). Specifically, when a search was conducted on the names or e-mail addresses of affected individuals using an Internet search engine, the search results would include links to the affected individuals’ résumés which had been uploaded to the Website. These résumés were accessible by clicking on the listed links.

2 The Organisation provided job seekers with the ability to upload their résumés on the Website so that the Organisation could assess their suitability for roles which the Organisation has been engaged to fill. The résumés would generally include personal data such as the name, phone numbers, employment history, educational qualifications, achievements and skill set of the job seekers. In one instance, it was discovered that a job seeker included additional information such as nationality, date of birth, marital status and current salary. (The personal data on the affected individuals’ résumés is collectively referred to as the “Personal Data”.)

3 The résumés uploaded to the Website were intended to only be accessible by recruitment agents employed by the Organisation. However, in practice, résumés which were uploaded to the Website were stored in a folder (“the Folder”) on the Website’s server which was not secured by access controls. As a result, these résumés were indexed by bot crawlers and could be found and accessed by the general public when a search was done via an Internet search engine.

4 The Organisation asserted to the Commission that it had instructed its third-party web developer (the “Developer”) to restrict access to the Folder to only one of the Organisation’s employees. However, the Organisation did not provide the Commission with any documentary evidence supporting its assertion and the Developer, in its statement to the Commission, denied receiving any specifications on security from the Organisation. Further, the Organisation had not conducted any checks or tests to ensure that access to the Folder was restricted or that the data in the Folder was encrypted. The Organisation admitted that the Developer had not processed any personal data on its behalf.

5 In its representations to the Commission, the Organisation stated that it had asked the Developer whether the résumés uploaded to the Website would be encrypted and the Developer responded saying that “it was safe”. This does not detract from the fact that the Organisation did not set out its instructions to the Developer in writing. As stated in *Re WTS Automotive Services Pte Ltd*,¹ when engaging a service provider, it is important for the organisation to clarify its obligations and thereafter document them in writing prior to the provision of services. As set out in *Re Smiling Orchid (S) Pte Ltd*:²

There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services.

1 [2019] PDP Digest 317 at [17].

2 [2017] PDP Digest 133 at [51].

6 Further, the Organisation's failure to conduct any checks on whether or not access controls were put in place was in itself a breach of its protection obligations: see *Re Tutor City*.³

7 The Organisation also asserted that it had relied on its web hosting and technical support services provider ("Web Host"), to ensure that the Website had adequate security features. However, the Organisation had not informed the Web Host that the contents of the Folder were meant to be protected. Hence, while the Web Host had performed some security reviews on the Website, it had not been engaged to advise on or implement measures to protect the personal data stored in the Folder.

8 After being informed of the Incident, the Organisation undertook the following remedial actions:

- (a) the Organisation requested the Web Host to assist in disabling the directory listing function of the Website;
- (b) the Organisation also engaged an external web developer to add a mechanism to the Website to help prevent future indexing by search engine crawlers;
- (c) public access permissions were removed from sensitive file directories to avoid similar incidents from recurring; and
- (d) the Organisation requested Google to remove the existing cached copies of the affected individuals' résumés from its search engine results.

FINDINGS AND BASIS FOR DETERMINATION

9 Section 24 of the Personal Data Protection Act 2012⁴ ("PDPA") requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control from unauthorised access, disclosure and similar risks. While the Organisation had outsourced the hosting of the Website to the Web Host, it remained in control of the Personal Data. Accordingly, the Organisation was responsible for making reasonable security arrangements to protect the Personal Data.

3 [2020] PDP Digest 170 at [16].

4 Act 26 of 2012.

10 The facts of this case, as set out above, clearly show the Organisation's failure to make reasonable security arrangements to protect the Personal Data. The cause of the Incident was that the Folder was set to allow access to documents within the Folder to the public without restrictions and the Organisation had not given the appropriate instructions to its contractors, including the Developer and the Web Host, to protect the Personal Data in the Folder.

11 As has been set out in numerous previous decisions issued by the Commission (see, for example, *Re Tutor City* ([6] *supra*)), one of the fundamental actions an organisation is required to undertake towards fulfilling its obligation to make reasonable security arrangements to protect personal data in its possession or under its control is to conduct relevant tests of its IT environment, including websites, to ensure that personal data has been adequately protected.

12 In the circumstances, I find the Organisation in breach of s 24 of the PDPA.

OUTCOME

13 Having found the Organisation in breach of s 24, I have decided to direct the Organisation to pay a financial penalty of \$7,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁵ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

14 Given the Organisation's remediation actions as set out above at [8], I have decided not to issue any other directions.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

5 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re i-vic International Pte Ltd

[2020] PDP Digest 485

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1804-B1991

Decision Citation: [2020] PDP Digest 485; [2019] SGPDPDC 41

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

12 November 2019

INTRODUCTION

1 The Employment and Employability Institute Ltd (“e2i”) administers a work trial programme on behalf of a public agency, Workforce Singapore (“WSG”). e2i engaged i-vic International Pte Ltd (the “Organisation”) to process claims and queries from members of the public relating to the work trial programme (the “Engagement”).

2 On 16 April 2018, e2i reported to the Personal Data Protection Commission (the “Commission”) that documents containing personal data of three individuals (the “Affected Individuals”) involved in the work trial programme were inadvertently attached to e-mails sent out by the Organisation to nine individuals (the “Incident”).

MATERIAL FACTS

3 As part of the Engagement, the Organisation was required to manage e2i’s mailbox which received e-mails from members of the public with their claims and queries. It was also required to develop and/or maintain the IT infrastructure and customer relationship management (“CRM”) software (collectively, the “System”) used to operate and manage e2i’s mailbox. As part of this, the Organisation was required to either reply to the e-mails from members of the public (providing the appropriate responses) or

escalate the queries in the e-mails to the relevant e2i representatives. Where an e-mail query needed to be escalated, an employee of the Organisation would submit an escalation request in the System. The System would then automatically generate two e-mails for the Organisation's employee to send (the "Automated E-mail Generation Process"). The first was a holding reply e-mail to the person who had sent the e-mail query to e2i's mailbox and the second was an e-mail to escalate the query to the relevant e2i representative. For the second e-mail, the System would automatically retrieve the relevant documents that were stored in the Organisation's servers and attach them to the e-mail.

4 On the first of every month, the Organisation ran a batch process on the System, after normal working hours, to generate reward programme e-mails for another client (the "Reward Programme Process"). While this was being done, the Automated E-mail Generation Process was unable to run any instructions to generate and send e-mails. During this time, any instructions by the Organisation's employees to generate e-mails with respect to the Engagement would be queued and the Automated E-mail Generation Process would process these instructions as a batch once the Reward Programme Process had been completed.

5 On 1 April 2019, while the Reward Programme Process was being run, one of the Organisation's employees attempted to generate some new e-mails using the Automated E-mail Generation Process. These instructions to generate the relevant e-mails were queued, to be acted upon only after the Reward Program Process was completed. However, due to an error in the Automated E-mail Generation Process code for processing e-mails as a batch, the System attached the wrong documents containing personal data of the Affected Individuals to the e-mails in the queue and sent these out to nine different individuals.

6 The documents that were sent to the nine individuals contained the names, NRIC numbers, signatures, residential addresses, mobile numbers, e-mail addresses, age and race of all three Affected Individuals, the bank account numbers of two of the Affected Individuals and the highest academic qualifications, work trial company details and work experience details of one of the Affected Individuals (collectively referred to as the "Disclosed Personal Data").

REMEDIAL ACTIONS BY THE ORGANISATION

7 After becoming aware of the Incident, the Organisation took the following remedial action to prevent it from reoccurring:

- (a) fixed the error in the code of the backlog clearing process which caused the Incident; and
- (b) rewrote the relevant code to enable automated encryption of attachments (so that unauthorised recipients would not be able to view the contents of the attachments) and to ensure that the wrong files would not be attached to e-mails.

FINDINGS AND BASIS FOR DETERMINATION

8 Section 24 of the Personal Data Protection Act 2012¹ (“PDPA”) provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the “Protection Obligation”).

9 As a preliminary point, it is noted that e2i was acting on behalf of WSG in relation to the collection, use and disclosure of personal data for administration of the work trial programme. As such, pursuant to s 4(1)(c) of the PDPA, e2i was not subject to Pts III to VI of the PDPA, including s 24, in relation to such collection, use and disclosure of personal data.

10 The Organisation was a data intermediary of e2i as it processed personal data on behalf of e2i for the purpose of the Engagement. The Organisation was thus required to protect personal data in its possession or under its control in accordance with s 24.

11 In relation to the cause of the Incident, the Organisation asserted that it had tested the code of the Automated E-mail Generation Process. However, the Organisation also admitted that it had not tested how the code acted when the Automated E-mail Generation Process processed instructions to generate and send e-mails which were queued while the Reward Programme Process was running. In this regard, the Organisation explained that it expected such e-mails to be processed and sent out individually and not queued while the Reward Programme Process was

1 Act 26 of 2012.

running. Nevertheless, as the Organisation ought to have known that the Automated E-mail Generation Process was unable to run while the Reward Programme Process was running on the first of every month, the Organisation ought to have tested whether this had an effect on the Automated E-mail Generation Process. Diligent and properly scoped testing would have simulated the circumstances leading to the Incident and would therefore likely have detected that documents containing personal data were being incorrectly attached to the e-mails in the queue.

12 In the circumstances, the Organisation's failure to put in place diligent and properly scoped testing amounted to a failure to put in place reasonable security arrangements to protect the personal data which was in its possession and/or under its control. I therefore find that the Organisation had contravened s 24 of the PDPA.

THE DEPUTY COMMISSIONER'S DIRECTIONS

13 In view of the above findings, I hereby direct the Organisation to pay a financial penalty of \$6,000 within 30 days from the date of this direction, failing which, interest at the rate specified in the Rules of Court² in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

14 I have decided not to issue any further directions as the Organisation has taken the actions set out at para 7 above to remedy the cause of the Incident.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

2 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re The Travel Corporation (2011) Pte Ltd

[2020] PDP Digest 489

Coram: Tan Kiat How, Commissioner

Case Number: DP-1810-B2821

Decision Citation: [2020] PDP Digest 489; [2019] SGPDPDC 42

Openness Obligation – Failure to designate one or more persons to be responsible for ensuring that organisation complied with Personal Data Protection Act 2012

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

19 November 2019

INTRODUCTION AND MATERIAL FACTS

1 The Travel Corporation (2011) Pte Ltd (the “Organisation”) offers travel packages both directly to Singapore customers and via third-party travel agencies. On 1 October 2018, the Organisation notified the Personal Data Protection Commission (the “Commission”) regarding the loss of a portable hard disk (the “Hard Disk”) which contained unencrypted files with the personal data of the Organisation’s customers, employees and suppliers (the “Incident”). The facts and circumstances of the Incident are as follows.

2 On 25 July 2018, a new employee of the Organisation left the office with her laptop and the Hard Disk; and misplaced both these devices on her way home. She initially only informed the Organisation about the loss of the laptop and a police report was made on 31 July 2018. The misplaced laptop did not contain any personal data. She eventually informed the Organisation about the loss of the Hard Disk on 21 September 2018 and the Organisation made another police report that day.

3 The table below summarises the number of affected individuals and their corresponding types of personal data contained in the Hard Disk:

S/N.	Category	Types of Personal Data in the Hard Disk	Number of Individuals Affected
1	Customers	Name, E-mail Address, Phone Number, Date of Birth and Postal Address	5,437
2		Same as item 1 plus Passport Number	21
3		Same as item 1 plus NRIC Number	242
4	Prospective Customers	Same as item 1	11,000
5	Employees	Name, Office E-mail Address and Office Phone Number	30
6	Suppliers	Names, Company Address, E-mail Address, Mobile Number, Office Number	1,900
Total number of individuals			18,630

4 It also emerged in the course of the Commission's investigations that the Organisation had not appointed any data protection officer ("DPO") prior to the data breach incident on 25 July 2018.

REMEDIAL ACTIONS BY THE ORGANISATION

- 5 The Organisation subsequently took the following remedial measures:
- (a) the Organisation ceased the use of portable storage devices and implemented the use of cloud-based storage for personal data in its possession; and
 - (b) the Organisation appointed a DPO on 22 October 2018.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had breached its obligation to protect personal data under section 24 of the Personal Data Protection Act 2012

6 Section 24 of the Personal Data Protection Act 2012¹ (“PDPA”) requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements. A review of the evidence disclosed that business contact information of the Organisation’s own employees and its suppliers comprised about 10% of the total number of affected individuals. Pursuant to s 4(5) of the PDPA, s 24 of the PDPA did not apply to such personal data. However, the personal data of the Organisation’s customers and prospective customers (the “Customers’ Personal Data”) have to be protected under the PDPA.

7 The Organisation failed to protect its Customers’ Personal Data as it failed to implement appropriate internal policies governing the use of portable storage devices containing personal data. While the Organisation has a Portable Computer and Storage Devices Policy that stipulated that “portable computing and storage devices used for business purposes must have designated custodians”, the Organisation did not have any operational frameworks or procedures in place that effectively implemented this policy in its individual business units. The Organisation only relied on verbal instructions to instruct its employees not to bring any portable storage devices out from the office premises. Further, the Organisation did not implement any password protection policies or data encryption policies for its portable storage devices, including the Hard Disk, although it had clear guidelines in its Acceptable User Policy and Information Sensitivity Policy to do so.

8 In the circumstances, the Commissioner found that the Organisation had not made reasonable security arrangements to protect its Customers’ Personal Data. The Organisation is accordingly in breach of s 24 of the PDPA.

1 Act 26 of 2012.

Whether the Organisation was in breach of section 11(3) of the Personal Data Protection Act 2012

9 Section 11(3) of the PDPA requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. Appointing a DPO is important in ensuring the proper implementation of an organisation's data protection policies and practices, as well as compliance with the PDPA: see, eg, *Re M Stars Movers & Logistics Specialist Pte Ltd.*²

10 As the Organisation failed to appoint a DPO prior to the data breach incident, the Commissioner found the Organisation in breach of s 11(3) of the PDPA.

THE COMMISSIONER'S DIRECTIONS

11 In view of the above findings, the Commissioner directs the Organisation to pay a financial penalty of \$12,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court³ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

12 In coming to this finding, the following mitigating factors were taken into account:

- (a) the Organisation notified the Commission of the Incident and fully co-operated with the Commission's investigations;
- (b) the Organisation promptly implemented remedial measures, as set out at [5] above, to address the breach;
- (c) the Organisation is actively addressing system security related recommendations provided by an external auditor; and
- (d) the Commission had not received any complaints as a result of the Incident.

13 In view of the remedial measures taken by the Organisation, the Commissioner decided not to impose any other directions.

2 [2018] PDP Digest 259 at [31]–[37].

3 Cap 322, R 5, 2014 Rev Ed.

The Organisation's representations

14 After the preliminary decision was issued to the Organisation, it made representations for a warning to be issued instead of an imposition of a financial penalty. The Organisation did not dispute the finding that it had breached s 24 of the PDPA.

15 In support of its request for a warning instead of the imposition of a financial penalty, the Organisation represented that it had taken the following rectification and remediation measures:

- (a) conducting a PDPA impact and gap analysis;
- (b) developing and enhancing internal PDPA policies and procedures;
- (c) improving current back-up systems and disaster recovery plans across the business promptly following the Incident;
- (d) notifying the affected individuals as soon as possible after the Incident;
- (e) filing a police report in case of potential misuse, ransom and/or other criminal activity;
- (f) arranging for PDPA training for employees;
- (g) publishing a privacy notice/statement on its website;
- (h) demonstrating proper co-ordination and practices in place; and
- (i) appointing a DPO.

16 The majority of the matters raised in mitigation are essentially remediation measures following from the gap analysis that the Organisation had performed. Due consideration had already been given to the prompt action that the Organisation took when the quantum of financial penalty was initially determined. None of the measures warrants an adjustment to the quantum of the financial penalty. Hence, the Organisation did not provide sufficient justification for the financial penalty to be replaced with a warning.

17 In its representations, the Organisation had provided an explanation for its failure to appoint a DPO. It had sent two employees to attend a data protection certification course. The Organisation explained that it did not appoint a DPO at the material time as its employees who attended the certified information privacy manager ("CIPM") course had failed to pass the CIPM examinations despite multiple attempts and the Organisation was under the impression that they could not be appointed as DPOs without passing the relevant examinations.

18 This misapprehension conflates the obligation to appoint a DPO and what is a reasonable way to go about it. The obligation for organisations to designate a DPO to ensure compliance with the PDPA under s 11(3) of the PDPA is a mandatory requirement under law. In the ideal case, the person appointed would be qualified to perform the role and undertake the responsibilities of a DPO at the time of appointment. The PDPA does not specify what these qualifications are. Furthermore, the pool of qualified DPOs, while growing, is small. There will be many instances where organisations will not be able to identify a member of staff or management who is already qualified. It is, therefore, perfectly acceptable to appoint a DPO and then send her for the necessary courses. In these situations, the Organisation should monitor the DPO's progress to ensure that there is no tardiness in completing the courses and achieving the requisite qualification.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re MSIG Insurance (Singapore) Pte Ltd and another

[2020] PDP Digest 495

Coram: Tan Kiat How, Commissioner

Case Number: DP-1708-B1066; DP-1708-B1086

Decision Citation: [2020] PDP Digest 495; [2019] SGPDPDC 43

Protection Obligation – Disclosure of personal data – Insufficient 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

19 November 2019

INTRODUCTION AND MATERIAL FACTS

1 MSIG Insurance (Singapore) Pte Ltd (“MSIG”) notified the Personal Data Protection Commission (the “Commission”) on 22 August 2017 that the mass e-mailing system of its service provider, Globalsign.in Pte Ltd (“GSI”), had been accessed without authorisation and used to send spam e-mails (the “Incident”) to 149,172 e-mail addresses which belonged to MSIG’s customers (“Impacted Customers”).

2 GSI runs and hosts an e-mail marketing platform known as “Global2Mail Online Marketing Web Application” (the “G2M” platform). GSI uses the G2M platform to send mass marketing e-mails to e-mail addresses supplied by its clients.

3 MSIG, an insurance provider, had engaged GSI to send marketing e-mails to its customers via the G2M platform. For this purpose, MSIG and GSI had entered into an agreement dated 1 October 2013. An addendum to the said agreement was entered into on 16 May 2014 to take into consideration the obligations of both organisations under the Personal

Data Protection Act 2012¹ (the “PDPA”). GSI’s services were renewed by MSIG, with MSIG and GSI entering into a new agreement on 1 August 2017 (the “Agreements”).

4 MSIG provided GSI with a list of e-mail addresses of its customers each time an e-mail marketing campaign was launched. For some of the e-mail addresses, MSIG also provided the first and last names to GSI and these would be captured on the G2M platform. According to MSIG, the e-mail addresses and names (where applicable) provided to GSI were password-protected.

5 Although no specific retention period for the e-mail addresses provided by MSIG to GSI was stated in the Agreements, MSIG required GSI to delete and purge the e-mail addresses and other personal data from its server after each marketing campaign. This is seen from e-mails sent by MSIG to GSI on 9 December 2016, 30 May 2017 and 5 June 2017 where MSIG asked GSI to confirm that it had purged the e-mail addresses which had been provided by MSIG to GSI for specific marketing campaigns.

6 On 18 August 2017, the administrator account of the G2M platform was accessed without authorisation. By accessing the administrator account, the intruder was also able to access the e-mail addresses and, in certain instances, names of individuals (the “Compromised Data”) that were stored on the G2M platform.

7 On 19 August 2017, the G2M platform sent spam e-mails to 359,364 e-mail addresses that were stored on the G2M platform (the “Spam E-mails”). Of these e-mail addresses, 149,172 were e-mail addresses of MSIG’s Impacted Customers (which MSIG had provided to GSI) and 201,192 were e-mail addresses of customers (“Other Impacted Individuals”) provided to GSI by three of GSI’s other clients for use with the G2M platform. Each of the Spam E-mails:

- (a) purported to provide tips on how to win a lottery;
- (b) contained a link under “clickbank.net” that redirected its users to a video on “lotterydominator.com”;
- (c) appeared to be sent from “MSIG Insurance” with the address “service@sg.msig-asia.com”;
- (d) was only sent to one e-mail address; and

1 Act 26 of 2012.

- (e) contained no other personal data other than the e-mail address of the recipient.

8 After MSIG informed the Commission about the Incident on 22 August 2017, MSIG and GSI jointly engaged a cybersecurity consultancy to investigate into the data breach.

9 The cybersecurity consultancy's investigations concluded that the Spam E-mails did not contain phishing or malware content. It would appear that the end users who clicked on the links in the Spam E-mails were simply redirected to the video on the "lotterydominator.com" website and there were no complaints from the users of any further negative consequences from clicking the links.

10 MSIG took the following remedial action after the Incident:

- (a) On 21 August 2017, MSIG posted an alert on the Spam E-mails on its corporate website and Facebook page.
- (b) On 22 August 2017, MSIG instructed GSI to purge all e-mail addresses and names of its customers in GSI's database, save for those customers that were affected, as it wanted to send out an apology e-mail.
- (c) FAQs were included from 28 August 2017. MSIG also instructed GSI to deactivate its e-mail account "service@sg.msiga-asia.com" which had been used to send the Spam E-mails.
- (d) On 24 August 2017, MSIG worked with GSI on an e-mail sent by the latter to all 149,172 affected MSIG customers to apologise for the breach. The e-mail included instructions on removing any malware from the link in the Spam E-mail. It provided a point of contact for any queries. MSIG instructed GSI to purge the e-mail addresses and names of its affected customers thereafter.

11 Between 21 and 30 August 2017, MSIG addressed queries from 92 customers who had been affected by the Incident.

12 Separately, GSI took the following remedial action after the Incident:

- (a) blocked the Spam E-mail link at server level to prevent recipients being redirected to the site;
- (b) immediately disabled the compromised administrator account to ensure no data would be exported and subsequently restored the account after putting in place additional security measures;

- (c) changed the password to the administrator account before restoring the account and implemented two-factor authentication (“2FA”) for all accounts whereby users would have to key in a one-time password sent either to their mobile number by SMS or Google Authenticator Application;
- (d) transferred the application database to a new server, hosted in Amazon Web Services in Singapore in an encrypted database;
- (e) enforced HTTPS so that all traffic from end users to GSI’s website would be encrypted;
- (f) improved logging of access, whereby IP addresses used to access G2M would be properly logged at application server level, and added logging of web attacks that had been blocked by the server firewall; and
- (g) engaged a consulting company to assist GSI in implementing policies that meet the ISO 27001 standards.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Compromised Data included personal data

13 The personal data found in the Compromised Data included (a) the first and last names of some MSIG customers; (b) the e-mail addresses of those customers (*ie*, which were stored with the names of the customers); and (c) the e-mail addresses of other customers which contained their full or partial names (the “Compromised Personal Data”). In relation to the latter set of e-mail addresses, as set out in *Re Credit Counselling Singapore*² (“*Re Credit Counselling*”), e-mail addresses are personal data if they disclose the full name or partial name of individuals which allows for the identification of such individuals.

14 The Compromised Data also included other e-mail addresses which were not linked to, or did not contain, the name of the customer (“Other E-mail Addresses”). It was also noted in *Re Credit Counselling* that an e-mail address coupled with other information which enables

2 [2018] PDP Digest 295 at [9].

identification of an individual, such as information obtained from a search on the Internet, is personal data.³

Whether MSIG or GSI had breached section 24 of the Personal Data Protection Act 2012

15 The main issue in this case is whether MSIG and GSI had done enough to protect the Compromised Personal Data which was in their possession or under their control. Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks.

16 As MSIG had provided the personal data relating to MSIG's Impacted Customers to GSI in order to make use of the G2M platform for its purposes, both MSIG and GSI are required to comply with s 24 of the PDPA. However, the scope of their respective obligations under that section differs. In addition, GSI would be required to comply with s 24 in respect of all Compromised Personal Data (that is, personal data relating to MSIG's Impacted Customers and the Other Impacted Customers).

17 In relation to MSIG, as it had engaged GSI to send marketing e-mails using the G2M platform, the scope of its obligations would relate to the arrangements MSIG established in order to ensure that GSI protected the personal data on the G2M platform. In respect of MSIG, the Commissioner found that MSIG had complied with its obligations under s 24 of the PDPA for the following reasons:

- (a) MSIG imposed security requirements on GSI under the Agreements to protect personal data. An express clause in the Agreements provides that GSI shall “implement sufficient and appropriate measures to guard against accidental or unauthorised access, collection, use, disclosure, misuse, loss, destruction, deletion, alteration, modification and processing of the Personal Data”.
- (b) MSIG also had the right under the Agreements to inspect and audit GSI.

3 *Re Credit Counselling Singapore* [2018] PDP Digest 295 at [10].

- (c) There was evidence that MSIG followed through with these contractual obligations with operational processes. For example, there were e-mails showing that MSIG required GSI to purge the personal data it provided after each marketing campaign. In this regard, MSIG had sent e-mails to GSI on at least three separate occasions between December 2016 and June 2017 asking GSI to purge e-mail addresses provided by MSIG from its system.

18 In relation to GSI, as GSI was operating the G2M platform, it was required to put in place reasonable security arrangements in the form of technical or administrative measures to protect the personal data on the G2M platform. In this regard, the Commissioner found that GSI had not made the appropriate security arrangements and was therefore in contravention of s 24 of the PDPA for the following reasons:

- (a) GSI had not implemented administrative or technical measures to require a regular change to the passwords to its administrator and client accounts on the G2M platform. In addition, GSI recognised that there was a risk that if accounts of staff who had left the employment of GSI were not disabled, these former staff may continue to have access to its applications. The need for an effective password expiry mechanism has been discussed in past decisions such as *Re Orchard Turn Developments Pte Ltd*⁴ (“*Re Orchard Turn Developments*”).
- (b) When the administrator account changed hands, there were no logs to record the fact that passwords had been changed.
- (c) Users were encouraged to choose strong passwords but GSI did not enforce any password strength requirements. The need for strong passwords is discussed in *Re Singapore Health Services Pte Ltd*.⁵
- (d) All the users of the administrator account shared the same administrator account and the same set of login credentials. This made it difficult to determine which member of staff had accessed the account or identify who had made changes to the system during each login session. *Re Orchard Turn Developments*

4 [2018] PDP Digest 223.

5 [2019] PDP Digest 376.

explains why the sharing of administrator account credentials can give rise to an increased risk of data breaches.

- (e) It was found that no security scans were carried out over the 12 months before the Incident. Security scans are important in the light of the type of personal data likely to be held by MSIG as an insurer. In *Re Courts (Singapore) Pte Ltd*,⁶ the Respondent's lack of regular testing and scanning for security issues were taken into account as factors to find a breach of s 24 of the PDPA.
- (f) GSI claimed that it had complied with MSIG's express instructions to "delete and purge the data after each marketing campaign". However, this cannot be true as the G2M platform still retained at least 149,172 e-mail addresses provided by MSIG which had been used in this Incident.

Whether GSI had complied with section 25 of the Personal Data Protection Act 2012

19 As noted above, it appeared that GSI had not deleted 149,172 e-mail addresses provided by MSIG after the relevant marketing campaigns were completed and notwithstanding e-mail reminders from MSIG. Section 25 of the PDPA requires an organisation to cease retaining documents containing personal data, or to 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 that personal data was collected is no longer being served by retention of the personal data; and
- (b) retention is no longer necessary for legal or business purposes.

20 As GSI was required to delete e-mail addresses provided by MSIG once the relevant marketing campaigns were completed, GSI *ipso facto* ceased to have any purpose for retaining the e-mail addresses on the G2M platform once the relevant marketing campaigns were completed. Accordingly, the Commissioner found that GSI was in contravention of s 25 of the PDPA.

6 [2019] PDP Digest 432.

GSI'S REPRESENTATIONS

21 After the Commissioner's preliminary decision was issued to MSIG and GSI, GSI submitted representations in relation to the quantum of financial penalty which the Commissioner proposed to impose in relation to its breach of s 24 of the PDPA and against the Commissioner's determination that it had breached s 25 of the PDPA. However, GSI did not disagree with, or make any representations relating to, the Commissioner's findings that it had breached s 24 of the PDPA.

22 First, GSI raised the following points as to why certain numbers of e-mail addresses should not be taken into consideration in determining the number of affected individuals:

- (a) 4,488 of the e-mail addresses which were stored on the G2M platform and which received the Spam E-mails did not include the name or any other identifier of the individuals;
- (b) approximately 12,000 Spam E-mails sent to the e-mail addresses stored on the G2M platform had bounced;
- (c) approximately 145,338 Spam E-mails were sent to GSI's overseas based clients; and
- (d) only 18,113 recipients opened the Spam E-mails and, of these, only 339 recipients clicked on the link contained within the Spam E-mails.

23 In relation to sub-para (a) above, the Commissioner accepts GSI's representation and has taken the reduced number of affected individuals into account in determining the financial penalty quantum specified below. In relation to (b), the fact that the Spam E-mails bounced is not conclusive that the e-mail addresses were invalid as the e-mails may have bounced due to other reasons, such as the recipient's e-mail inbox being full at that time. In relation to (c), GSI is required to protect personal data in its possession or under its control and it is immaterial whether the relevant individuals were resident in Singapore or overseas. Finally, in relation to (d), it has already been taken into account that there was no harm suffered by the recipients (see [32] below) and the Organisation's point at (d) above does not provide further mitigation of the Organisation's breach.

24 Secondly, GSI represented that MSIG had access to the G2M platform and could exercise functions such as verifying the content of the platform, creating and sending out e-mail campaigns and deleting content and e-mails. However, the fact that MSIG had access to the G2M platform

does not absolve GSI from its obligations under the PDPA. The fact remains that MSIG had engaged GSI to send marketing e-mails using the G2M platform and GSI was obliged under the PDPA to protect the personal data that was in its possession or under its control for the purposes of this engagement. Furthermore, MSIG had specifically instructed GSI to delete the e-mail addresses after each marketing campaign and this is something that GSI is contractually bound to do.

25 Thirdly, GSI raised the following additional points as mitigating factors for the Commission's consideration:

- (a) GSI had been fully co-operative during the Commission's investigations;
- (b) there was no evidence of exfiltration, further disclosure or modification of the Compromised Data;
- (c) the Spam E-mails sent to the Impacted Customers did not contain any personal data;
- (d) there was no evidence of actual loss or damage suffered by any of the Impacted Customers;
- (e) GSI has also sent an e-mail notification to all Impacted Customers of the Spam E-mails;
- (f) GSI has in place internal data protection policies prior to the Incident; and
- (g) GSI has since taken further steps to tighten and strengthen its data protection policies and mechanisms, including sending additional employees for further PDPA training, engaging external vendors to conduct advisory sessions and gap analysis, completing a surveillance audit and implementing various internal programmes and workshops to promote data responsibility.

26 The matters in sub-paras (a) to (d) above had already been taken into consideration in determining the financial penalty (see [32] below). With regard to (f), organisations are required under the PDPA to implement policies and practices necessary for them to meet their obligations under the PDPA, and mere compliance with the PDPA is not a mitigating factor.

27 GSI's notification of the affected individuals is a relevant consideration and the further steps set out in (g) are relevant mitigating factors and the quantum of the final financial penalty set out below has been reduced.

28 Fourthly, GSI sought to compare the facts of this case with prior decisions such as *Re Avant Logistic Service Pte Ltd*,⁷ *Re AIA Singapore Private Limited*,⁸ *Re InfoCorp Technologies Pte Ltd*,⁹ *Re Option Gift Pte Ltd*¹⁰ and *Re AIG Asia Pacific Insurance Pte Ltd*.¹¹ It should be borne in mind that none of these cited cases dealt with a similar scale of breach and cannot be relied upon to argue for a lower financial penalty.

29 GSI also made the following representations against the Commissioner's determination that it had breached s 25 of the PDPA:

- (a) GSI sent an e-mail to MSIG on 5 June 2017 confirming the deletion or purging of data from previous campaigns. This e-mail read as follows:

Yes, we are in the midst of purging the most recent campaigns. The older ones have been purged.

The above e-mail does not confirm that all completed campaigns have been purged, and only indicated that GSI was in the midst of doing so, and shows that some e-mail addresses from recently concluded campaigns had not been removed from the system. This is, at best, evidence that GSI was trying to purge customer data after each campaign but was not particularly prompt.

- (b) GSI asserted that MSIG was an active client and, hence, the G2M platform retained 149,172 e-mail addresses of MSIG's customers even after data from previous campaigns had been purged. However, this is contrary to the evidence which shows that MSIG had requested GSI to delete all e-mail addresses after each e-mail marketing campaign; and GSI's representations that it was putting in effort to do so (albeit with some delays).

In the final analysis, the representations in relation to the breach of s 25 of the PDPA did not warrant a review of the Commissioner's findings.

7 [2020] PDP Digest 371.

8 [2020] PDP Digest 298.

9 [2020] PDP Digest 282.

10 [2020] PDP Digest 219.

11 [2019] PDP Digest 363.

OUTCOME

30 After considering the facts of this case, the Commissioner hereby directs GSI to pay a financial penalty of \$34,000 within 30 days from the date of the directions, failing which, interest shall be payable on the outstanding amount of such financial penalty at such rate as specified in the Rules of Court.¹²

31 In determining the amount of the financial penalty set out above, the Commissioner recognised that not all of the 359,364 e-mail addresses targeted by the Spam E-mails in the Incident constituted personal data and it was not possible for the Commission to determine the exact number of e-mail addresses which did constitute personal data. Nevertheless, taking into account the GSI lapses and the other facts of the case detailed above, the Commissioner considered that a financial penalty of \$34,000 would be appropriate.

32 In coming to this decision, the Commissioner also had regard to the following mitigating factors:

- (a) GSI was co-operative in the course of the Commission's investigation and had provided prompt responses to the Commission's requests for information;
- (b) GSI implemented the remedial actions set out at [10] to [12] above to address the Incident quickly, including notifying the affected individuals; and
- (c) there was no harm caused by the disclosure of the Compromised Personal Data.

33 The Commissioner was of the view that no further directions are required given the remedial actions already taken by MSIG and GSI.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

12 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re Chizzle Pte Ltd

[2020] PDP Digest 506

Coram: Tan Kiat How, Commissioner

Case Number: DP-1807-B2495

Decision Citation: [2020] PDP Digest 506; [2019] SGPDPDC 44

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

26 November 2019

INTRODUCTION

1 Chizzle Pte Ltd (the “Organisation”) provides a mobile application (the “Mobile App”) designed to connect learners and teachers in Singapore, Australia and India. On 31 July 2018, the Organisation notified the Personal Data Protection Commission (the “Commission”) of a cyberattack (the “Incident”) which had compromised the personal data of about 2,213 users of the Mobile App, including some users in Singapore (the “Affected Individuals”).

MATERIAL FACTS

2 On 30 July 2018, the Organisation noticed that the Mobile App had stopped responding. It was found that an unauthorised party had deleted its database containing the personal data of the Affected Individuals (the “Chizzle Database”) and left a ransom demand in text. The personal data in question included the names, dates of birth, genders, e-mail addresses and some mobile numbers and residential addresses of the Affected Individuals (the “Compromised Personal Data”). Before this, on 9 July 2018, the Organisation had changed the Chizzle Database from Amazon’s Relational Database Service to the MySQL relational database.

3 Since 2016, the Organisation had a “L.A.M.P.” stack (*ie*, Linux operating system, Apache HTTP server, MySQL server and PHP) (collectively with the Mobile App, the “System”) as part of its IT infrastructure. “phpMyAdmin”, a MySQL database administration tool, was installed with the L.A.M.P stack. The tool was configured to allow remote access to it from the Internet. The Organisation believed that the unauthorised party gained entry into the Chizzle Database through the phpMyAdmin tool by a brute force attack. However, it did not have the logs to prove that a brute force attack had taken place. Regardless, the unauthorised party gained entry to the Chizzle Database through the phpMyAdmin tool. This gave the unauthorised party full control, including reading, writing and deleting data.

REMEDIAL ACTIONS BY THE ORGANISATION

4 Following the Incident, the Organisation has taken measures to prevent unauthorised access to the Chizzle Database in the future, including the following:

- (a) IP address access via phpMyAdmin (*ie*, use of IP address to find and reach the Chizzle Database) was turned off and the phpMyAdmin tool was uninstalled;
- (b) the IP address of the Organisation’s servers, including the Chizzle Database server, were changed; and
- (c) the Mobile App and Chizzle Database were moved to new hardware in case any residual malware or Trojans remained in the old hardware.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had breached its obligation to protect personal data under section 24 of the Personal Data Protection Act 2012

5 Section 24 of the Personal Data Protection Act 2012¹ (“PDPA”) requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent

1 Act 26 of 2012.

unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

6 The Organisation had failed to conduct any security review of its System although past decisions by the Commission had made clear the need for such reviews.²

7 The Organisation claimed that it was not even aware that the phpMyAdmin tool was part of its System. It also claimed it had no need of the tool. A reasonable security review would have included a review of all web-connected features of the System. Through such a review, the Organisation would have found the phpMyAdmin tool and could have decided whether to remove or keep it. If the Organisation had decided to retain the tool, the review would have given the Organisation an opportunity to review its security against web-based threats.

8 However, as found above, the Organisation failed to conduct a security review. It therefore missed the opportunity to determine its need for the phpMyAdmin tool and to address the security requirements of the tool, if retained. A security review would have been the arrangement through which the Organisation could reasonably have prevented the unauthorised entry into the Chizzle Database through the tool.

9 On the facts above, the Commissioner found that the Organisation had not made reasonable security arrangements to protect the Compromised Personal Data and was accordingly in breach of s 24 of the PDPA.

THE ORGANISATION'S REPRESENTATIONS

10 After the preliminary decision was issued, the Organisation submitted representations requesting for a reduction in the quantum of financial penalty. In support of its assertion that the proposed penalty was “more than likely to push [it] to a brink of closing the business”, the Organisation submitted copies of its financial statements and bank account statements. The Organisation did not disagree with, or make any representations

2 See, eg, *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317; *Re Bud Cosmetics Pte Ltd* [2019] PDP Digest 351; and *Re Watami Food Service Singapore Pte Ltd* [2019] PDP Digest 221.

relating to, the Commissioner's findings that it had breached s 24 of the PDPA.

11 In general, financial penalties imposed under the PDPA reflect the seriousness of the breach and do not take into account the financial position of the organisation in question. However, a financial penalty is not meant to impose a crushing burden on the organisation and cause undue hardship.³ In the present case, the financial standing that was gleaned from the submitted financial statements and bank account statements was dire. In order to avoid imposing a crushing burden on the Organisation, the Commissioner has decided to reduce the financial penalty. For this reason, the financial penalty imposed in this case should not be taken as establishing a precedent for future cases.

12 In order to ensure that the Mobile App is robust and secure, the Organisation should adopt a data protection by design approach. While the optimal approach is to do so from the commencement of every developmental project, it is nevertheless still possible to do so during the maintenance phase, whenever there are enhancements: Data Protection by Design Guide, at p 35.⁴ The Organisation is directed to review its developmental processes in order to adopt a data protection by design approach for future enhancements to the Mobile App. Making changes to its practices will help the Organisation scale its Mobile App for future growth, and will pay longer-term dividends than a hefty financial penalty.

THE COMMISSIONER'S DIRECTIONS

13 In view of the above findings, the Commissioner decided to direct the Organisation to pay a financial penalty of \$8,000 within 30 days from the date of this direction, failing which, interest at the rate specified in the Rules of Court⁵ in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

3 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [34].

4 Personal Data Protection Commission and Privacy Commissioner for Personal Data, Hong Kong, *Guide to Data Protection by Design for ICT Systems* (31 May 2019).

5 Cap 322, R 5, 2014 Rev Ed.

14 In addition, the Commissioner decided to issue the following directions to the Organisation to ensure its compliance with the PDPA:

- (a) engage duly qualified personnel to conduct a security audit of its mobile application and accompanying IT system;
- (b) furnish a schedule stating the scope of risks to be assessed and the time within which a full report of the audit can be provided to the Commission within 30 days of this direction;
- (c) rectify security gaps identified in the security audit;
- (d) develop an IT security policy to guide its employees on the security of personal data on its mobile applications and accompanying IT systems within 60 days from the date of completion of the above-mentioned security audit;
- (e) within 120 days of this decision, review and revise its developmental processes in order to adopt a data protection by design approach for future enhancements to its mobile application; and
- (f) inform the Commission in writing of the completion of each of the above directions within one week of completion.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

Grounds of Decision

Re SAFRA National Service Association

[2020] PDP Digest 511

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1809-B2711

Decision Citation: [2020] PDP Digest 511; [2019] SGPDPDC 45

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

16 December 2019

FACTS OF THE CASE

1 On 13 September 2018, the Personal Data Protection Commission (the “Commission”) received a voluntary breach notification from SAFRA National Service Association (the “Organisation”). An employee of the Organisation (the “Employee”) had sent out two separate batches of e-mails attaching an Excel spreadsheet (the “Spreadsheet”) containing the personal data of certain members of the Organisation’s shooting club (the “SSC”) to other members (the “Incident”).

2 According to the Employee, his job scope included sending mass e-mails to SSC members. He has been sending such e-mails since September 2016 at least once a month. According to him, he was not aware of any standard operating procedures for sending such mass e-mails. The Employee claims that his supervisor had instructed him verbally on the process. First, prepare proposed e-mail, and attach a spreadsheet containing intended recipients’ e-mail addresses extracted from another internal system. Next, send this draft e-mail from his individual work e-mail account to the official SSC e-mail account. Thereafter, copy the intended recipients’ e-mail addresses into the draft e-mail, and delete the attached spreadsheet, before sending out the mass e-mail. This is the process that the Employee has been following whenever he sends mass e-mails to SSC members, as was the case during the Incident.

3 The Organisation claims that it was not aware of this process for mass e-mails. However, its staff were briefed on the practice of using the “bcc” function when sending mass e-mails and were verbally instructed to “check and ensure that no unnecessary information or document (including those which contain personal data) has been enclosed before sending an email to members”.

4 The Incident occurred on 9 September 2018. The Employee followed this procedure to publicise an upcoming event. After copying the e-mail addresses from the Spreadsheet and pasting them in the “bcc” field of the e-mail, the Employee tried to delete the Spreadsheet. He was prompted by the webmail that “the attachment could not be removed and to try again”. This was the first time he encountered such an error message. The Employee claims that upon trying to delete the Spreadsheet again, “the Spreadsheet disappeared from the email draft” and he proceeded to send the first batch of mass e-mails. The same thing happened for the second batch of mass e-mails sent by the Employee. According to the Employee, he was notified by an SSC member right after sending the second batch of mass e-mails that the Spreadsheet had been attached to the mass e-mails. Upon checking the “Sent Items” folder on the SSC e-mail account, he realised that the Spreadsheet was attached in the sent e-mails.

5 The Incident resulted in the Spreadsheet containing the personal data of 780 SSC members being sent to 491 SSC members. The types of personal data in the Spreadsheet (the “Personal Data”) included the following:

- (a) name;
- (b) NRIC number;
- (c) date of birth;
- (d) address;
- (e) telephone number; and
- (f) e-mail address.

6 Upon being notified of the Incident, the Organisation took the following remedial actions:

- (a) completed the masking of members’ NRIC numbers in its internal systems and reports, which it was in the process of undertaking;

- (b) circulated the Commission’s guidelines on the Personal Data Protection Act 2012¹ (the “PDPA”) with reminders to be mindful when handling personal data;
- (c) notified all affected SSC members about the Incident via e-mail and SMS, and provided an e-mail address and phone number for members to contact for any queries about the Incident;
- (d) put up an announcement on the Organisation’s website regarding the Incident;
- (e) set up an incident response team and incident management hotline and prepared an FAQ document for its frontline staff; and
- (f) followed up with phone calls to the SSC members who received the Spreadsheet to delete the attachment.

FINDINGS AND BASIS FOR DETERMINATION

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

8 As a preliminary point, the Organisation alleges that it had replicated the steps taken by the Employee to confirm whether or not the Employee’s version of events was accurate. The Organisation claimed that, in replicating these steps, it had similarly encountered the issue as set out at [4] above. When the Commission requested for evidence of the tests conducted, the Organisation provided some screenshots of e-mails with attachments, and stated that the test results were not saved, although “[the investigation team] had witnessed [the test] but no screen shot or video recording was made”. However, these screenshots were inconclusive in demonstrating that the Organisation managed to replicate the issues. As part of its investigations, the Commission contacted the Organisation’s webmail software service provider who informed that it had not encountered such an issue nor had it encountered or received any enquiry on such an issue from users of its webmail software at the material time. On a balance of probabilities, based on a review of the evidence before me, I am

1 Act 26 of 2012.

unconvinced that there was a software glitch. It is more likely that the Employee had simply failed to delete the attached Spreadsheet prior to sending the e-mails out.

9 The key issue in this case revolves around the practice adopted by the Organisation for sending mass e-mails. The Organisation's method of drafting the mass e-mail using the individual work e-mail address of the relevant employee and then sending it to the official SSC e-mail address with the Spreadsheet attached gave rise to the risk of accidental disclosure of the Personal Data in the Spreadsheet. Manual processes such as this give rise to risks of human error. Having in mind that this is a task that the Employee had to perform at least once a month, and the fact that the Organisation had already digitised its membership records, the task could have been partially automated. There are readily available technical solutions like mail-merge functions or the creation of frequently used mailing lists. The Commission's *Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data*² states that organisations may implement automated processing of documents or communications containing personal data (eg, merging content or populating fields from various sources) to ensure destination information is correct. Organisations are also reminded to ensure the accuracy and reliability of the automated processing implemented by checking these systems and processes regularly.

10 Further, the Commission's *Guide for Printing Processes for Organisations*³ also provides guidance on how organisations may use mail merge when e-mailing to ensure the accuracy of the list of intended recipients and the corresponding merged fields in the e-mail.

11 Additionally, the Organisation was unaware of this manual process that its Employee had been using since September 2016 (and potentially earlier, by other employees or by his supervisor) to send out mass e-mails. As stated at [3] above, the Organisation claimed that it had given certain verbal instructions to its staff on data protection handling practices pertaining to e-mail correspondence. In general, verbal instructions are insufficient as employees would be unable to refer to them in the course of their duties and may very well be unable to recall such instructions after some time. For a regular and perhaps even frequent task like the present

2 Published 20 January 2017, at para 2.1.

3 Published 3 May 2018, at p 11.

monthly mass e-mail to members to publicise upcoming events, the Organisation should have a properly documented process and consider the use of process automation tools.

12 In the light of the foregoing, I am satisfied that the Organisation had contravened s 24 of the PDPA.

13 The Organisation informed the Commission after the preliminary decision in this matter was issued to the Organisation that the following measures have since been put in place:

- (a) Mass e-mails will no longer be sent using the Organisation's generic e-mail account and will only be sent out by a designated executive or authorised personnel approved by the club manager using his or her individual work e-mail account.
- (b) The downloading of the list of members from the Organisation's system will be carried out by the executive personally.
- (c) The categories of personal data in the list of members that may be downloaded from the system have been reduced.
- (d) The frequency of mass e-mails to update members on programmes and events will be reduced from monthly to bi-monthly or quarterly.
- (e) All new staff will undergo an orientation programme on the operations of the shooting club within the first week of joining and only selected staff will be allowed to handle e-mail updates and will also be trained within the first week of joining the club.
- (f) More stringent access controls to the Organisation's databases have been implemented.
- (g) The first five characters of members' NRIC numbers are masked in the Organisation's internal systems.
- (h) The IT policy has been updated to include guidelines for the protection, encryption and sharing of the Organisation's database. As part of this update, databases are to be encrypted or password protected before they are shared and may only be shared with the written consent of a head of department or custodian.
- (i) Training has been provided to staff on data handling.

14 The Organisation also informed that it was in the midst of enhancing its existing system to automate the sending of mass e-mails. The

Organisation asked for an extension of the time frame for implementation of the second direction set out in the next section. The Deputy Commissioner has decided to accede to the Organisation's request and has lengthened the time frame to the period set out below.

THE DEPUTY COMMISSIONER'S DIRECTIONS

15 In determining the directions to be imposed on the Organisation under s 29 of the PDPA, I took into account the following mitigating factors:

- (a) the Organisation voluntarily notified the Commission of the Incident;
- (b) the Organisation was co-operative and had provided prompt responses to the Commission's requests for information;
- (c) the Organisation implemented remedial actions swiftly to address the Incident; and
- (d) there was no evidence of any further unauthorised use of the Personal Data in the Spreadsheet.

16 Having carefully considered all the relevant factors of this case, I hereby direct the Organisation:

- (a) to pay a financial penalty of \$10,000 within 30 days of the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁴ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full; and
- (b) to conduct a review of its e-mail system and processes to put in place process safeguards and written internal standard operating procedures to protect the personal data of its members within 120 days of the date of this direction.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

4 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re National Healthcare Group Pte Ltd

[2020] PDP Digest 517

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1802-B1703; DP-1802-B1765

Decision Citation: [2020] PDP Digest 517; [2019] SGPDPDC 46

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

26 December 2019

INTRODUCTION

1 On 10 February 2018, the National Healthcare Group Pte Ltd (the “Organisation”) notified the Personal Data Protection Commission (the “Commission”) about a complaint it had received in relation to a list containing personal information of partner doctors of the Organisation (the “List”) which was accessible on the Internet (the “Incident”). Subsequently, on 28 February 2018, the Commission received a separate complaint over the Incident.

FACTS OF THE CASE

2 On 17 March 2015, the Organisation awarded a developer (“Website Developer”) a contract to develop its website (the “Website”). The Organisation specified the Website’s functional requirements and contents. A company specialising in IT services (“IT Services Provider”) provided the Organisation with IT support. In this regard, the IT Services Provider ensured that the IT specifications of the Organisation were complied with by the Web Developer, which included co-ordinating and verifying bug fixes and remedies of security vulnerabilities implemented by the Web Developer. During the process of developing the Website, a section for

restricting access to the Website (including the List) was not included in a web configuration file.¹ The Organisation, Website Developer and IT Services Provider signed off on the Website's functional requirements specification, user acceptance test cases, and website commissioning. The relevant web configuration file was not examined before the Website went "live" in December 2015.

3 Around June or July 2016, a vendor (the "Vendor") was engaged to conduct a penetration test of the Website. The penetration test report (the "Penetration Test Report") highlighted the unrestricted access to the List through the Internet as a vulnerability. The Penetration Test Report also recommended the remedy, which was to ensure that the authorisation rules be configured to restrict Internet access to authorised users only.

4 On 7 February 2018, a general practitioner ("GP"), who had signed up to be a partner doctor of the Organisation, found the List through a Google search of her name and notified the Organisation. The List contained personal information of 129 GPs who had registered to be partner doctors of the Organisation via an online form on the Website ("NHG Partners"), and personal information of five members of the public which was generated when they submitted feedback on the Website.

5 The types of information contained in the List (collectively, the "Disclosed Data") include:

- (a) With respect to the 129 GPs:
 - (i) their full names (128 GPs), mobile numbers (111 GPs), mailing addresses (14 GPs), e-mail addresses (117 GPs) and clinic addresses (115 GPs) (collectively, "GP's Contact Information");
 - (ii) Singapore Medical Council ("SMC") registration numbers of 129 GPs ("GP's Registration Numbers"); and
 - (iii) NRIC numbers (111 GPs), dates of birth (112 GPs) and photographs (41 GPs) (collectively, "GP's Other Data").

1 Web configuration files determine the way a website or directory on a website behaves. Web configuration files placed in the root directory of a website will affect the behaviour of the entire site.

- (b) With respect to the five non-GPs, full names and e-mail addresses, as well as mobile numbers of three of them (“Other Individual’s Data”).

6 Upon being notified of the Incident on 7 February 2018, the Organisation promptly carried out the following remedial actions:

- (a) On 8 February 2018, the Organisation took the Website offline, as well as found and fixed the cause of the Incident.
- (b) The Organisation sent several requests to Google to remove cached copies of the List indexed from 9 to 13 February 2018. From 21 February 2018, the Organisation performed daily Google searches on the 129 affected records until the cached links could no longer be found on 5 March 2018. Thereafter, the Organisation conducted periodic Google searches until 8 May 2018.
- (c) From 19 February 2018 to 6 March 2018, the Organisation contacted all affected GPs to inform them of the Incident.

7 In addition, to prevent a recurrence of a similar Incident, the Organisation has also adopted the following practices:

- (a) Two additional checks at front-end publishing site for SharePoint websites will be carried out during user acceptance test and prior to going “live”:
 - (i) the project manager would check for configuration which controls publishing of “visible” pages (lists) after the vendor submits the web configuration prior to the deployment; and
 - (ii) the test script would include testing of authorised access to the relevant web pages. The web pages would also generally be tested to ensure non-public web pages cannot be accessed by non-authorised users.
- (b) Performing penetration tests prior to websites going “live”.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Protection Obligation under section 24 of the Personal Data Protection Act 2012 applies to the Disclosed Data

8 While the Disclosed Data is personal data as defined in s 2(1) of the Personal Data Protection Act 2012² (“PDPA”), the Protection Obligation under s 24 did not apply to the following two categories of Disclosed Data – GP’s Contact Information and GP’s Registration Numbers.

9 In relation to GP’s Contact Information, pursuant to s 4(5) of the PDPA, Pts III to VI of the PDPA do not apply to business contact information. GP’s Contact Information falls within the definition of “business contact information” as defined in s 2(1) of the PDPA because it was provided by the GPs to the Organisation for the purposes of registration as NHG Partners, and as a means of contacting them in their professional capacity.

10 In relation to GP’s Registration Numbers, the same information is generally available to the public on the SMC website and hence it is “publicly available” as defined in s 2(1) of the PDPA. The *raison d’être* for making such information available is to assist in the identification of licensed medical practitioners and the nature of their qualification and practice. The register of medical practitioners is maintained by the SMC under s 19 of the Medical Registration Act.³ It is maintained as multiple lists, *ie*, locally-trained doctors, international medical graduates, provisional, conditional, temporary or full registrations, as well as specialist registration and family physician registration. This information enables an inquisitive patient to verify the nature of medical practice that a physician is permitted to practise. To my mind, this is information that falls under the “other similar information about the individual” limb of the definition of business contact information as it assists in the identification of the medical practitioner to whom the business contact information relates.

11 In the circumstances, the Protection Obligation only applied to GP’s Other Data and Other Individual’s Data (collectively, the “Disclosed Personal Data”).

2 Act 26 of 2012.

3 Cap 174, 2014 Rev Ed.

Whether the Organisation had breached the Protection Obligation under section 24 of the Personal Data Protection Act 2012

12 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.

13 As a preliminary point, the Organisation owned the Website and had possession and control over the Disclosed Personal Data at all material times. While the Website Developer was engaged to develop the Website and the IT Services Provider provided IT support to the Organisation (including maintenance and technical support for the Website), the investigations revealed that neither of these parties processed the Disclosed Personal Data on the Organisation's behalf with respect to the Website. The IT Services Provider and Website Developer were accordingly not data intermediaries with respect to the operation of the Website, and the Organisation was solely responsible for the protection of the Disclosed Personal Data.

14 Based on the investigations, the Organisation had failed to put in place reasonable security arrangements to protect the Disclosed Personal Data as explained below.

15 The Penetration Test Report expressly pointed out that web services could be used to access SharePoint data (which included the List containing the Disclosed Personal Data) via the Internet and recommended that this vulnerability be remediated by reconfiguring the web configuration to restrict access to authorised users only. The Penetration Test Report was issued more than a year prior to the Incident. This was more than sufficient time for the Organisation to remedy the vulnerability which caused the Incident.

16 According to the Organisation, the vulnerability was inadvertently left unfixed as it was not sufficiently highlighted by the Vendor in the Penetration Test Report. This was an unsatisfactory excuse. First, the relevant findings and recommendations were the first item in the Penetration Test Report. Second, they were expressed in terms that no technical expertise was required for their significance to be understood. If the Organisation did not understand the findings and/or recommendations, it should have consulted the Vendor for clarification.

17 The Organisation also asserted that it had relied on the IT Services Provider and Website Developer to act on any issues identified in the Penetration Test Report. It should be reiterated that while an organisation may delegate work to vendors to comply with the PDPA, the organisation's responsibility for complying with its statutory obligations under the PDPA may not be delegated.⁴ In this case, the Organisation failed to exercise reasonable oversight with respect to the review of the Penetration Test Report and rectification of the vulnerabilities of its Website.

REPRESENTATIONS BY THE ORGANISATION

18 In the course of settling this decision, the Organisation made representations and asked that a warning be imposed in lieu of a financial penalty. The Organisation raised the following factors in its representations:

- (a) As the appointed public healthcare shared services provider, the IT Services Provider was responsible for the overall management, deployment and maintenance of the Organisation's IT systems, including the Website. Similar to the facts of *Re Singapore Health Services Pte Ltd*,⁵ the IT Services Provider's staff was deployed to the Organisation to support day-to-day operations and provide technical support. As there was no IT staff employed by the Organisation, it had to rely on the technical expertise provided by the IT Services Provider. In particular, the Chief Information Officer ("CIO") and Cluster Information Security Officer ("CISO") for the Organisation was employed by the IT Services Provider and seconded to the Organisation.
- (b) The IT Services Provider was a data intermediary. The Website's database was hosted on the Healthcare Data Centre (H-Cloud) network which was (and is still) operated, maintained and managed by the IT Services Provider.
- (c) The IT Services Provider was in charge of the penetration test, as well as co-ordinating and deploying the fixes. The

4 See *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [14] and [23].

5 [2019] PDP Digest 376.

vulnerability in the Website that caused the Incident was not highlighted to the Organisation.

- (d) The Disclosed Personal Data was not medical data, and therefore not personal data of a particularly sensitive nature which should be accorded a higher standard of protection.

19 Having considered the representations, I have decided to maintain the financial penalty set out at [21] below for the following reasons:

- (a) While the IT Services Provider's staff deployed to fill the CIO and CISO roles may have been employed by the IT Services Provider, to the extent that they were carrying out the functions of the Organisation's CIO and CISO in accordance with the terms of their secondment, they were acting on behalf of the Organisation. As such, I find that their actions should be attributed to the Organisation and not the IT Services Provider.
- (b) The Incident did not arise from a compromise of the Healthcare Data Centre (H-Cloud) network that hosted the Website's database. Instead, and as mentioned at [2] above, the cause of the Incident was that a section for restricting access to the Website (including the List) was not included in a web configuration file. While the IT Services Provider provided technical support for the Website, it did not process the Disclosed Personal Data through the Website. The IT Services Provider was accordingly not a data intermediary with respect to operation of the Website.
- (c) As explained at [15] to [17] above, the Organisation failed to exercise reasonable oversight with respect to review of the Penetration Test Report and rectification of vulnerabilities of the Website. In this regard, the Penetration Test Report had expressly pointed out that web services could be used to access SharePoint data (which included the List containing the Disclosed Personal Data) and recommended that this vulnerability be remediated by reconfiguring the web configuration to restrict access to authorised users only.
- (d) The fact that the Disclosed Personal Data was not medical data had already been taken into account in the quantum of financial penalty set out at [21] below, which would have been higher if the Disclosed Personal Data had been of a more sensitive nature, such as medical data.

DIRECTIONS

20 In determining the directions, if any, to be imposed on the Organisation under s 29 of the PDPA, I took into account the following mitigating factors:

- (a) the Organisation took prompt remedial actions following the Incident as set out at [6] and [7] above;
- (b) the Organisation was fully co-operative during the investigations;
- (c) the Organisation took immediate steps to notify the affected individuals of the Incident; and
- (d) there was unauthorised disclosure to one individual and no modification or exfiltration of the Disclosed Personal Data.

21 Having considered all the relevant factors of this case, I hereby direct the Organisation to pay a financial penalty of \$6,000 within 30 days from the date of the directions, failing which, interest, at the rate specified in the Rules of Court⁶ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full. I have not set out any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

6 Cap 322, R 5, 2014 Rev Ed.

Grounds of Decision

Re PeopleSearch Pte Ltd

[2020] PDP Digest 525

Coram: Yeong Zee Kin, Deputy Commissioner

Case Number: DP-1903-B3521

Decision Citation: [2020] PDP Digest 525; [2019] SGPDPDC 47

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

26 December 2019

INTRODUCTION

1 PeopleSearch Pte Ltd (the “Organisation”) is a subsidiary of a listed Singapore company (“Listed Company”) that provides professional recruitment and flexible staffing services in Asia. On 15 March 2019, the Listed Company notified the Personal Data Protection Commission (the “Commission”) of a ransomware attack suffered by the Organisation on 1 to 2 March 2019, which resulted in the Organisation not being able to access its clients’ personal data (the “Incident”).

FACTS OF THE CASE

2 At the material time, the Organisation had a business division that managed outsourced payroll for the Organisation’s clients. In order to do so, the Organisation used a payroll software installed in a server in a virtual machine environment (the “VM Server”). The Organisation’s clients would connect to the VM Server through remote desktop protocol to use the payroll software. All the information (including personal data) in the payroll software was stored in a database that was hosted in the VM Server.

3 At the time of the Incident, the database included the following personal data of 472 individuals employed by two of the Organisation's clients¹ (collectively, "Employee Data"):

- (a) name;
- (b) NRIC number;
- (c) residential address;
- (d) contact number;
- (e) e-mail address;
- (f) bank account number; and
- (g) salary details.

4 The database also included the following personal data of the employees' next of kin ("Next of Kin Data"):²

- (a) name;
- (b) age;
- (c) contact number; and
- (d) relationship to the respective individual.

5 Taking into consideration the individuals whose information was stored as Next of Kin Data, it is estimated that a total of 944 individuals (comprising the 472 individuals with Employee Data and 472 individuals with Next of Kin Data) were affected by the Incident (the "Affected Individuals").³

1 The payroll information of the Organisation's other clients had been migrated from the VM Server to another server. This was in preparation for the Organisation's business division managing outsource payroll being incorporated into a separate legal entity.

2 Some or all of the Next of Kin Data may also constitute Employee Data in that it may be data about the employee (namely, who is their next of kin) which may enable the employee to be identified. However, as the total number of Affected Individuals includes both the employees and their next of kin, the two sets of data are identified separately for the purposes of this decision.

3 The Organisation was unable to provide the Personal Data Protection Commission with the number of individuals who were listed as "next of kin" in the payroll information of the 472 individuals as it was no longer in possession of the relevant customer data file. It is estimated that each of the 472 individuals would have provided Next of Kin Data of at least one individual.

6 The Organisation discovered the Incident on 4 March 2019 when a ransom note appeared when it attempted to access the VM Server. The ransom note informed the Organisation that its files had been encrypted and required payment in bitcoins in exchange for the decryption key. The Organisation refused to pay the ransom to the cyberattacker and restored its business operations by using a backup of the VM Server as at 1 March 2019.

7 Upon discovery of the Incident, the Organisation promptly carried out the following remedial actions:

- (a) disabled remote desktop accounts and/or changed passwords to mitigate any risks relating to credentials; and
- (b) installed the latest windows server updates on the restored VM Server.

8 Based on the Organisation's internal investigations, there was no spike in the outgoing traffic logs from the VM Server at the time of the Incident. This suggested that the risk that Employee Data (including the Next of Kin Data) was exfiltrated by the cyberattacker was immaterial. On 1 April 2019, the Organisation's business division managing outsource payroll was incorporated into a separate legal entity and the VM Server was decommissioned.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had breached section 24 of the Personal Data Protection Act 2012

9 It is undisputed that Employee Data and Next of Kin Data constitute "personal data" as defined in s 2(1) of the Personal Data Protection Act 2012⁴ (the "PDPA"). The Organisation had possession and/or control over the Employee Data and Next of Kin Data at all material times, and accepted its responsibility for protecting such data under the PDPA. While there may have been no exfiltration of the Employee Data, as mentioned at [8] above, there was unauthorised modification of the Employee Data as the ransomware rendered it inaccessible to the Organisation.

4 Act 26 of 2012.

10 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. In assessing the standard of reasonable security arrangements required, I considered the fact that Employee Data included NRIC numbers and personal data of a financial nature (*ie*, bank account numbers and salary details).⁵ When it comes to the protection of such 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 an unauthorised use of such data.⁶ In my view, the Organisation failed to put in place reasonable security arrangements to protect the Employee Data and Next of Kin Data for the reasons explained below.

11 The Organisation admitted that it had not carried out any security scans, penetration testing or patching of the VM Server for at least 12 months preceding the Incident. According to the Organisation, its omission was due to the departure of an employee who was responsible for oversight of the VM Server. This explanation is not accepted.

12 As emphasised in previous decisions and the Commission's *Guide to Securing Personal Data in Electronic Medium*,⁷ regular security testing and patching of IT systems are important security measures that organisations should implement to guard against a possible intrusion or attack.⁸ The Organisation's failure to have any process in place to ensure regular security testing and patching of the VM Server resulted in a system that had vulnerabilities and gaps that were exploited by the attacker in planting the ransomware to encrypt the Employee Data. In view of the fact that the VM Server stored personal data of a sensitive nature, this fell far short of the standard of protection required. In the circumstances, I find the Organisation in breach of s 24 of the PDPA.

13 Nevertheless, I note that the Organisation had a good practice of having regular backups of the VM Server. This significantly mitigated the

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

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

7 Revised 20 January 2017, at paras 16.3 and 16.4.

8 See, for example, *Re Genki Sushi Singapore Pte Ltd* [2020] PDP Digest 347 at [20] and [21].

impact of the Incident on the Organisation's business operations. The Organisation was able to restore the VM Server from a backup as at 1 March 2019, and only lost access to the Employee Data for approximately two days from 2 March 2019 to 4 March 2019.

14 In today's digital age where organisations store information (including personal data) online and move towards a paperless future, it is critically important that they have processes in place to back up their data at frequent and regular intervals. The failure to do so may result in crippling consequences to an organisation's business operations in the event of a cyberattack. In this case, the Organisation's good practice of having regular backups is a strong mitigating factor that I have taken into account in determining the quantum of financial penalty to impose.

THE DEPUTY COMMISSIONER'S DIRECTIONS

15 Having found the Organisation in breach of s 24 of the PDPA, I took into account the following mitigating factors in determining the directions to be imposed on the Organisation:

- (a) the Organisation's regular backup process of the VM Server which significantly mitigated the impact of the Incident as discussed at [13] and [14] above;
- (b) the Organisation's prompt actions to mitigate the effects of the Incident and prevent recurrence of a similar breach;
- (c) the Organisation's full co-operation with the Commission's investigations;
- (d) there did not appear to be any exfiltration of Employee Data from the VM Server; and
- (e) the Commission did not receive any complaints about the Incident and there was no indication that the Incident caused harm to the Affected Individuals.

16 Having considered all the relevant facts and circumstances of this case, I hereby direct the Organisation to pay a financial penalty of \$5,000 within 30 days from the date of this direction, failing which, interest, at the rate specified in the Rules of Court⁹ in respect of judgment debts, shall accrue

9 Cap 322, R 5, 2014 Rev Ed.

and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
Deputy Commissioner
For Personal Data Protection

Grounds of Decision

Re Society of Tourist Guides (Singapore)

[2020] PDP Digest 531

Coram: Tan Kiat How, Commissioner

Case Number: DP-1903-B3445

Decision Citation: [2020] PDP Digest 531; [2019] SGPDPDC 48

Accountability Obligation – Failure to appoint data protection officer

Accountability Obligation – Lack of data protection policies and practices

Protection Obligation – Unauthorised access and disclosure of personal data –

Insufficient security arrangements

26 December 2019

INTRODUCTION

1 On 3 March 2019, the Personal Data Protection Commission (the “Commission”) received a complaint that personal data of individuals had apparently been exposed to unauthorised access and disclosure through links on the Society of Tourist Guides (Singapore)’s (the “Organisation”) website.

FACTS OF THE CASE

2 The Organisation is a non-profit organisation that works with the Singapore Tourism Board (“STB”) to promote the professionalism of tourist guides as tourism ambassadors of Singapore. Tourist guides registered with STB may sign up as members of the Organisation (“Members”). In May 2018, the Organisation engaged a Vietnam-based IT company (the “Vendor”) to develop its website <<https://societyoftouristguides.org.sg>> (the “Website”).

3 One of the Organisation’s purposes for the Website was to collect personal data from its Members. Personal data was collected from Members through their respective user accounts on the Website and included their

names, photographs, contact numbers, e-mail addresses and a write-up of themselves (for example, with the type of services they provided) (“Profile Data”). Members could also upload images of their identification documents (eg, NRIC, employment pass, driving and vocational licences) which contained various personal data (“ID Data”).

4 Members’ Profile Data was published on their respective public profile pages on the Website. This enabled members of the public to find and engage a Member with the necessary experience and expertise to provide services that he or she required.

5 As regards the ID Data, this was used by the Organisation for a few purposes. These included (a) applying for SkillsFuture grants for training programmes conducted for Members; (b) facilitating arrangements for Members to gain access to secure locations when required (eg, transit areas in airports); and (c) verifying that the Members were qualified to provide transport services based on his or her driving and vocational licences.

6 The Organisation did not specify any requirements to its Vendor with respect to the storage and protection of Members’ personal data collected through the Website. The Website was launched on 1 October 2018. Since its launch, the Organisation has been managing the Website, with the Vendor’s role limited to *ad hoc* technical assistance.

7 On 3 March 2019, the Commission received a complaint that there had been disclosure without consent of sensitive information of individuals, such as Singapore NRIC, driving licence and photographs, through links on the Website (the “Incident”). The Commission’s investigations revealed that a total of 111 unique Members were affected by the Incident (the “Affected Members”).¹ In this regard, the publicly accessible directories on the Website (“Web Directories”) were found to store images of identification documents set out below which contained ID Data of the Affected Members (the “Disclosed Data”):

1 A Member could have uploaded images of more than one type of identification document on the Website.

S/N.	Type of Identification Document	Type of Personal Data in the Identification Document	Number of Members Affected
1	NRIC	Name, NRIC number, photograph, thumbprint, address, date of birth, country of birth, race, gender and date of issue.	97
2	Singapore Armed Forces Identity Card	Name, NRIC number/colour, photograph, address, date of birth, country of birth, race, gender, blood group, service status and military rank status.	1
3	Vietnamese Identity Card	Name, card number, photograph, date of birth, place of birth, place of residence, fingerprints, ethnic group, religion and date of issue.	1
4	Singapore Employment Pass	Name, photograph, occupation, Foreign Identification Number, date of application, date of issue, date of expiry and employer.	1
5	Singapore Driving Licence	Name, licence number (same as NRIC number), photograph, date of birth, classes of vehicles the individual is licensed to drive and each pass date and date of issue.	47
6	Singapore Vocational Licence	Name, licence number (same as NRIC number), photograph, date of issue and type and description of each vocational licence held, and their respective dates of issue.	16

8 It also emerged in the course of the Commission’s investigations that the Organisation had not appointed any data protection officer (“DPO”), and had not developed and put in place any data protection policies that are necessary for it to meet its obligations under the Personal Data Protection Act 2012² (the “PDPA”).

9 Following the Incident, the Organisation took the following remedial actions:

2 Act 26 of 2012.

- (a) appointed two DPOs;
- (b) with the assistance of its Vendor, disabled public access to the Web Directories and contacted Google to remove all cached images of the Disclosed Data; and
- (c) developed a data protection policy.

FINDINGS AND BASIS FOR DETERMINATION

Whether the Organisation had contravened section 24 of the Personal Data Protection Act 2012

10 As a preliminary point, the Organisation owned and managed the Website, and had possession of and control over the Disclosed Data at all material times. While the Vendor had been engaged to develop the Website and subsequently provided technical assistance on an *ad hoc* basis, the Vendor had not processed any personal data collected via the Website on the Organisation's behalf. The Vendor was therefore not a data intermediary of the Organisation, and the Organisation was solely responsible for the protection of the Disclosed Data under the PDPA.

11 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.

12 In this regard, the Commissioner found that the Organisation had failed to put in place reasonable security arrangements to protect the Disclosed Data for the following reasons. First, as mentioned at [6] above, the Organisation did not specify any requirements to its Vendor with respect to the storage and protection of personal data (including the ID Data) which was collected from Members through the Website. The Organisation had intended for the Website to have public profile pages on which Members' Profile Data was displayed for public access, but at the same time ID Data was collected and to be used for administrative purposes like applying for training grants, facilitating access to secure location and verifying driving qualifications. Clear requirements could and should have been communicated to its Vendor that ID Data collected through the Website was not meant to be publicly accessible. This can be done by the Organisation from the perspective of the business owner of the Website,

while relying on the Vendor to propose the technical implementation that will meet this business requirement.

13 The Commission's investigations also revealed that security testing had never been conducted since the launch of the Website in October 2018. In this regard, the Organisation admitted that it failed to take into consideration the security arrangements of the Website due to its lack of experience. As observed in *Re WTS Automotive Services Pte Ltd*,³ while an organisation may not have the requisite level of technical expertise, a responsible organisation would have made genuine attempts to give proper instructions to its service providers. The gravamen in the present case was the Organisation's failure to do so.

14 The Commission's *Guide on Building Websites for SMEs*⁴ provides guidance on what is expected from organisations contracting professional services to build their corporate websites or other online portals. In particular, organisations that engage IT vendors to develop and/or maintain their websites should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms.⁵

15 Secondly, and as observed in *Re Tutor City*,⁶ where documents containing personal data have to reside on web servers, folder or directory permissions are common and direct methods of controlling access and preventing unauthorised access by public users and web crawlers. Depending on its business needs and circumstances, the Organisation could have instructed the Vendor to implement any of the following reasonable technical security measures to protect the Disclosed Data:

- (a) Place documents containing the Disclosed Data in a non-public folder/directory.
- (b) Place documents containing the Disclosed Data in a non-public folder or directory, with access to these documents controlled through web applications on the server.
- (c) Place documents containing the Disclosed Data in a sub-folder within the public directory but control access to files by creating

3 [2019] PDP Digest 317 at [24].

4 Revised 10 July 2018.

5 Personal Data Protection Commission, *Guide on Building Websites for SMEs* (revised 10 July 2018) at para 4.2.1.

6 [2020] PDP Digest 170 at [21]–[23].

a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (eg, implement a password requirement or an IP address restriction).

16 In view of the above, the Commissioner found that the Organisation had contravened s 24 of the PDPA.

Whether the Organisation was in breach of sections 11(3) and 12 of the Personal Data Protection Act 2012

17 In relation to the Organisation's failure to appoint a DPO and develop and implement any data protection policy, these are required under ss 11(3) and 12, respectively, of the PDPA. In particular, s 11(3) requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. Section 12 of the PDPA requires organisations to (among other things):

- (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; and
- (b) communicate information about such policies to its staff.

18 The importance of these requirements has been emphasised multiple times in previous decisions. For example, it is important for an organisation to document its data protection policies and practices in writing as they serve to increase awareness and ensure accountability of the organisation's obligations under the PDPA (*Re Aviva Ltd*).⁷ Similarly, appointing a DPO is important in ensuring the proper implementation of an organisation's data protection policies and practices, as well as compliance with the PDPA (see, eg, *Re M Stars Movers & Logistics Specialist Pte Ltd*).⁸

19 In the circumstances, the Organisation was clearly in breach of ss 11(3) and 12 of the PDPA. While it has since appointed DPOs, it has not yet developed written policies and practices necessary to ensure its compliance with the PDPA.

7 [2018] PDP Digest 245 at [32].

8 [2018] PDP Digest 259 at [31]–[37].

REPRESENTATIONS BY THE ORGANISATION

20 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose and requested that the financial penalty be paid in instalments. The Organisation raised the following factors for the Commissioner's consideration:

- (a) the Organisation had limited funds in its bank account and does not have any tangible assets which may be sold to raise funds to pay the financial penalty;
- (b) the Organisation had been making losses in the preceding three months; and
- (c) the Organisation had been seeking funding assistance from the STB.

21 Having carefully considered the representations, the Commissioner has decided to maintain the financial penalty set out at [23(a)] below. The matters raised by the Organisation at [20] above are not additional mitigating factors that justify a reduction in the financial penalty. However, the Commissioner is agreeable to the Organisation's request that the financial penalty be paid in instalments.

THE COMMISSIONER'S DIRECTIONS

22 In determining the directions, if any, to be imposed on the Organisation under s 29 of the PDPA, the Commissioner took into account the following mitigating factors:

- (a) the Organisation was co-operative in the investigations and provided information promptly;
- (b) upon being notified of the Incident, the Organisation took action to disable public access to the Web Directories, and notified its Members of the Incident; and
- (c) there was limited unauthorised access and disclosure of the Disclosed Data as the Web Directories had only been accessed a total of six times.

23 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to:

- (a) Pay a financial penalty of \$20,000 in eight instalments by the due dates as set out below, failing which, the full outstanding amount shall become due and payable immediately and interest, at the rate specified in the Rules of Court⁹ in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full:
- (i) first instalment of \$2,500 on 1 February 2020;
 - (ii) second instalment of \$2,500 on 1 March 2020;
 - (iii) third instalment of \$2,500 on 1 April 2020;
 - (iv) fourth instalment of \$2,500 on 1 May 2020;
 - (v) fifth instalment of \$2,500 on 1 June 2020;
 - (vi) sixth instalment of \$2,500 on 1 July 2020;
 - (vii) seventh instalment of \$2,500 on 1 August 2020; and
 - (viii) eighth instalment of \$2,500 on 1 September 2020.
- (b) Complete the following within 60 days from the date of this direction:
- (i) review the security of the Website and implement appropriate security arrangements to protect the personal data in its possession or control;
 - (ii) put in place written internal policies and practices as required under s 12 of the PDPA;
 - (iii) develop and implement a training policy for employees of the Organisation handling personal data to be trained to be aware of, and to comply with the requirements of, the PDPA when handling personal data; and
 - (iv) require all existing employees to attend such training.

YEONG ZEE KIN
Deputy Commissioner
For Commissioner for Personal Data Protection

9 Cap 322, R 5, 2014 Rev Ed.

Case Summary

RE BARNACLES PTE LTD

Protection Obligation – Disclosure of personal data – Insufficient 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

1 Barnacles Pte Ltd (the “Organisation”) operates a website which enables its customers to make reservations to dine at its restaurant. For this purpose, it collected certain personal data from its customers such as their name, contact number, e-mail address and date and time of their reservation, amongst other information (the “Personal Data”). However, when the Organisation developed its website, the Organisation did not instruct the vendor it appointed to develop the website to implement security arrangements to protect the Personal Data. The Organisation also made no effort to verify whether any security arrangements had been put in place by its appointed vendor. As a result, the Personal Data was accessible over the Internet, for example, if a search was made on a customer’s name using an Internet search engine. The Organisation ceased operations in January 2019 but continued to retain the Personal Data until May 2019, even though it did not have any legal or business purpose to retain the Personal Data other than to fulfil or decline its customers’ reservations.

2 Following a complaint against the Organisation in April 2019, the Personal Data Protection Commission found that the Personal Data of 149 individuals had been exposed to the risk of unauthorised disclosure as a result of the Organisation’s failure to make security arrangements to protect the Personal Data and/or to cease to retain the Personal Data once it no longer had any legal or business purpose to retain it. In the circumstances, the Deputy Commissioner for Personal Data Protection found the

Organisation in breach of ss 24 and 25 of the Personal Data Protection Act 2012¹ and decided to give a warning to the Organisation.

1 Act 26 of 2012.

Case Summary

RE CAMPVISION LTD

Protection Obligation – Unauthorised access to and disclosure of personal data – Insufficient security arrangements

1 CampVision Ltd (the “Organisation”) engaged SHINE Children and Youth Services (“SHINE”) to collect evaluation feedback from youths participating in its programmes. For this purpose, SHINE collected information from the youths on the Organisation’s behalf, including their names, NRIC numbers, e-mail addresses and schools (the “Personal Data”). SHINE did this using a platform provided by Typeform SL (“Typeform”), a company based in Spain, which provides online survey services. In June 2018, Typeform discovered that an unknown third party had gained access to its server and downloaded information provided by many Typeform users, including the Personal Data collected by SHINE on behalf of the Organisation (the “Incident”).

2 The Personal Data Protection Commission (the “Commission”) found that the Personal Data of 106 individuals collected by SHINE on behalf of the Organisation had been exposed to the risk of unauthorised access and disclosure in the Incident. The Commission’s investigations revealed that there was no written contract between the Organisation and SHINE setting out SHINE’s obligations with respect to the processing and protection of the Personal Data, which it collected on the Organisation’s behalf. The Organisation also admitted that it had not conveyed any instructions to SHINE with respect to protection of the Personal Data. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ and decided to give a warning to the Organisation.

1 Act 26 of 2012.

Case Summary

RE ERGO INSURANCE PTE LTD

Protection Obligation – Disclosure of personal data – Insufficient security arrangements

1 ERGO Insurance Pte Ltd (the “Organisation”) is a general insurer and operates an Internet portal (the “Portal”) which enables its insurance intermediaries, who are not the Organisation’s employees, to request for documents of policyholders represented by the intermediaries. These documents contain the policyholders’ personal data such as their names, addresses, car registration numbers, genders, nationalities, NRIC numbers, dates of birth and contact numbers (the “Personal Data”).

2 The Organisation voluntarily informed the Personal Data Protection Commission on 15 October 2018 that it had earlier discovered, on 11 September 2018, that some of its insurance intermediaries had been incorrectly sent documents of policyholders who were represented by other insurance intermediaries (the “Incident”). The Incident arose when some insurance intermediaries (the “Intermediaries”) requested for documents of policyholders whom they represent through the Portal. However, the Organisation’s application and printer servers had been shut down for a scheduled system downtime and when they were restarted, the Organisation’s employees had failed to follow the correct restart process. They were supposed to start both servers at the same time, but this was not done as the starting of the printer server initially failed. This resulted in documents with duplicate document IDs being generated and hence the wrong documents being sent to the Intermediaries. As a result of the Incident, the Personal Data of 57 individuals were mistakenly disclosed to the Intermediaries.

3 The Personal Data Protection Commission found that the Organisation did not have in place a clearly defined process to restart its application and printer servers and a sufficiently robust document ID generation process (such as including a timestamp as part of the document ID) to prevent the duplication of document IDs. In the circumstances, the

Deputy Commissioner for Personal Data Protection found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ and decided to give a warning to the Organisation. No directions are required as the Organisation implemented corrective measures that addressed the gap in its security arrangements.

1 Act 26 of 2012.

Case Summary

RE GLOBAL OUTSOURCE SOLUTIONS PTE LTD

Accountability Obligation – Lack of data protection policies and practices
Protection Obligation – Unauthorised access to and disclosure of personal data – Insufficient security arrangements

1 Global Outsource Solutions Pte Ltd (the “Organisation”) provided warranties for products purchased by its clients’ customers. To be eligible for this warranty, customers registered their purchases with the Organisation via the Organisation’s website¹ (the “Website”). The Organisation collected various personal data from such customers for this purpose, including personal information such as their name, e-mail address, mailing address and contact number, and details of the customers’ purchases such as the name of the product purchased, the purchase date, the name of the retailer and the location of the physical store where the product was purchased (collectively, the “Personal Data”).

2 The Personal Data Protection Commission (“the Commission”) received a complaint on 23 September 2018 that the complainant could access the Personal Data of another individual when viewing a warranty registration summary page on the Website (the “Incident”).

3 The Organisation admitted to the occurrence of the Incident but was unable to identify the cause of the Incident. The Commission found that the Organisation had not provided any security requirements to the vendor it had engaged sometime in 2013 to develop the Website. Consequently, it had not reviewed the Website’s security arrangements or conducted any security testing on the Website. In the circumstances, the Organisation had not implemented reasonable security arrangements to protect the personal data collected by the Website (including but not limited to the Personal

1 At <<http://www.globaloutsourcelandia.com>>.

Data disclosed in the Incident) and is therefore in breach of s 24 of the Personal Data Protection Act 2012² (the “PDPA”).

4 The Commission also found that the Organisation did not have any internal data protection policies for its employees in relation to the handling of personal data for the purposes of registering products through the Website. This failure to develop and implement such internal data protection policies is a breach of s 12 of the PDPA.

5 The Organisation has since removed the warranty registration section on its Website and is in the process of revamping its Website to incorporate the necessary security arrangements. The Organisation is directed to develop and implement policies for data protection and staff training in data protection, and to put all employees handling personal data through data protection training.



2 Act 26 of 2012.

Case Summary

RE HONESTBEE PTE LTD

Protection Obligation – Unauthorised access to personal data – Lack of access control

1 Honestbee Pte Ltd (the “Organisation”) is an online food and grocery delivery service. Third-party merchants, which either engaged or were planning to engage the Organisation for delivery services, provided it with personal data of their customers in order to test its logistics service delivery platform. The Organisation stored this personal data in its Amazon Web Services (“AWS”) file repository. The personal data (the “Personal Data”) included names, e-mail addresses, residential addresses and mobile numbers.

2 The Personal Data Protection Commission (the “Commission”) was informed on 2 May 2019 that the Personal Data was accessible to the public. The number of individuals whose personal data was accessible was about 8,000. The Organisation admitted that it had mistakenly placed the Personal Data in a “bucket” (which is similar to a file folder) without access restrictions. This allowed anyone with knowledge of AWS’s command line to gain access to the Personal Data.

3 The Commission found that the Organisation omitted to put in place the most rudimentary security measures necessary to protect the Personal Data. For example, the Organisation could have implemented a requirement to conduct checks to confirm that any personal data used in testing was stored in a “bucket” with the appropriate access restrictions. In the circumstances, the Organisation had not implemented reasonable security arrangements to protect the Personal Data and was therefore in breach of s 24 of the Personal Data Protection Act 2012.¹

4 The Organisation has since blocked public access to the Personal Data by modifying the relevant access settings and circulated a report to its

1 Act 26 of 2012.

engineering team to ensure that similar mistakes would not be repeated in code reviews. The Organisation is also in discussions with cybersecurity companies to perform regular security audits on its systems.

5 The Organisation is directed to pay a financial penalty of \$8,000 within 30 days from the date of this direction, failing which interest at the rate specified in the Rules of Court² in respect of judgment debts shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full. In view of the remedial measures taken by the Organisation, the Commission has not imposed any other directions.

6 The Organisation's prompt co-operation in the course of the Commission's investigation, its prompt actions taken to remediate the breach and the limited unauthorised disclosure of the Personal Data were mitigating factors taken into consideration in determining the quantum of the financial penalty.

2 Cap 322, R 5, 2014 Rev Ed.

Case Summary

RE ICLICK MEDIA PTE LTD

Accountability Obligation – Lack of data protection policies and practices

1 Following a complaint against EU Holidays Pte Ltd (“EU Holidays”), the Personal Data Protection Commission (the “Commission”) conducted an investigation to determine whether EU Holidays had contravened the Personal Data Protection Act 2012¹ (the “PDPA”). In the course of investigations, it was found that EU Holiday’s IT vendor, iClick Media Pte Ltd (the “Organisation”), had not developed any internal policies and practices that are necessary for it to meet its obligations under the PDPA. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of s 12 of the PDPA and decided to direct the Organisation to, within 60 days:

- (a) put in place a data protection policy, including written internal policies, to comply with the provisions of the PDPA;
- (b) develop a training programme for the Organisation’s employees in respect of their obligations under the PDPA when handling personal data and require all employees to attend such training; and
- (c) by no later than seven days after the above actions have been carried out, the Organisation shall, in addition, submit to the Commission a written update.

1 Act 26 of 2012.

Case Summary

RE SATURDAY CLUB PTE LTD

Accountability Obligation – Lack of data protection policies and practices

1 Upon investigation into a suspected data breach, it was found that Saturday Club Pte Ltd (the “Organisation”) had not developed any internal policies and practices that are necessary for it to meet its obligations under the Personal Data Protection Act 2012¹ (“PDPA”). In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of s 12 of the PDPA and decided to issue directions to the Organisation.

1 Act 26 of 2012.

Case Summary

RE TAN TOCK SENG HOSPITAL PTE LTD

Protection Obligation – Unauthorised disclosure of personal data – Insufficient security arrangements

1 Tan Tock Seng Hospital Pte Ltd (the “Organisation”) voluntarily informed the Personal Data Protection Commission (the “Commission”) on 14 February 2019 that it had discovered on 12 February 2019 that letters sent to 85 patients (the “Affected Individuals”) to reschedule their appointments with the Organisation (the “Letters”) had been sent to the wrong addresses (the “Incident”). These Letters contained the names, NRIC numbers and appointments of the Affected Individuals (the “Personal Data”). Such letters were usually generated automatically. However, on 12 February, the Letters were generated manually using the mail merge function in Microsoft Word to extract the Personal Data from a spreadsheet (the “Spreadsheet”) and insert the data in the letters. However, the staff that had been tasked to generate these letters only selected and sorted the address field in the Spreadsheet. As a result, the addresses in the Spreadsheet no longer corresponded to the correct patient information and when the staff ran the mail merge function, the incorrect addresses were inserted in the letters.

2 The Commission found that the Organisation did not conduct any checks on the generation and printing of the letters. A simple random sampling of the letters would have likely averted the Incident or greatly reduced the number of individuals affected. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of s 24 of the Personal Data Protection Act 2012¹ and decided to give a warning to the Organisation. No directions are required as the Organisation has implemented corrective measures that addressed the gap in its security arrangements.

1 Act 26 of 2012.

