PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 6

Case No DP-2007-B6646

In the matter of an investigation under section 50(1)
of the Personal Data Protection Act 2012

And

Farrer Park Hospital Pte Ltd

… *Organisation*

DECISION

Data Protection *– Protection Obligation – Unauthorised access to personal data - Unauthorised disclosure of personal data – Failure to implement reasonable security arrangements – Email auto-forwarding*

Data Protection *– Financial penalty – Voluntary admission of liability*

Farrer Park Hospital Pte Ltd

[2022] SGPDPC 6

Lew Chuen Hong, Commissioner — Case No. DP-2007-B6646

15 September 2022

Introduction

1 On 23 July 2020, the Personal Data Protection Commission (the "**Commission**") received a data breach notification from Farrer Park Hospital Pte Ltd (the "**Organisation**"). The Organisation discovered that between 8 March 2018 and 25 October 2019, 9,271 emails had been automatically forwarded from two employees' (the "**Employees**") Microsoft Office 365 work email accounts (the "**Email Accounts**") to a third-party's email address (the "**Third Party**"), thereby disclosing the personal data of 3,539 unique individuals (the "**Incident**").

Background

2 The Organisation is a private tertiary healthcare institute that provides a range of healthcare services. The nature of the Organisation's operations requires its employees to regularly handle highly sensitive personal data of past, present, and prospective patients. At the material time, the Employees were part

of the Organisation's marketing department which, *inter alia*, processes requests for the Organisation's medical services via email. The email requests received by the Organisation's marketing department contain personal data pertinent to the medical treatment(s) requested by individuals including:

(a) Name;

(b) Gender;

(c) Nationality;

(d) Date of Birth;

(e) NRIC Number (full and partial);

(f) Passport details (including Passport numbers);

(g) Contact number;

(h) Photograph; and

(i) Medical information, including the following (the "**Medical Information**"):

(i) Medical Condition(s) – namely, patient's health condition(s), including doctor's diagnosis, brief description of the health condition provided by the patient or an appointment with a specialist for a specific condition mentioned;

(ii) Medical History – namely, more than one record of a patient's health condition(s).

(iii) Medical Results/Reports – namely, documents containing a medical procedure or analysis (for example, X-Rays).

(collectively, the "**Affected Data Types**")

Security measures prior to discovery of the Incident

3 At the time of the Incident, the Organisation had implemented various IT and data protection policies regulating the collection, use, disclosure, and protection of personal data, including:

(a) A '*Data Protection Handbook*' to provide awareness and assistance to its employees in complying with the Personal Data Protection Act 2012 (the "**PDPA**");

(b) A '*Personal Data Protection Policy for Patient Records*' to outline the Organisation's protocol for managing patients' medical records as well as the relevant retention period of medical records;

(c) An '*IT Security Management Standards*' policy detailing the establishment, implementation, and management of the Organisation's information security program to ensure the prevention, detection, containment, and correction of security breaches;

(d) An '*Access Control Standards*' policy setting out the Organisation's standards relating to user accounts and password security settings; and

(e) An '*Acceptable Use Policy*' stipulating the Organisation's rules governing the acceptable use of its IT resources, including access to emails, websites, the internet, and other types of organisational information, and which mandated that user passwords be at least 8 characters long, and contain characters from at least 3 of the below 4 categories

(i) "*English upper-case letters (e.g., A, B, C, ...Z)*";

(ii) "English lower-case letters (e.g., a, b, C, ...Z)";

(iii) "Alphanumeric (e.g., 1, 2, 3, ...9)"; and

(iv) "Special characters) (e.g., ?, !, %, $, #)".

4 The Organisation had also implemented various IT security measures and vendor-based solutions including:

(a) Staff training sessions on medical confidentiality, and periodic email updates on developments to the PDPA and guidelines issued by the Commission;

(b) Regular phishing exercises on employees to continually inculcate awareness on the techniques that malicious actors might deploy to undermine the organisation's IT security;

(c) A cloud-based filtering service to protect the Organisation against spam, malware, and other email threats;

(d) Signature-based and behaviour-based endpoint protections to protect endpoints from known and unknown malicious files;

(e) User and entity behaviour analytics utilising deep learning algorithms to identify anomalies based on the Organisation's usual network traffic;

(f) Webpage whitelisting solutions to only allow users to access permitted sites and/or category of sites based on the Organisation's defined policies;

(g) Firewalls to prevent unauthorised access into FPH's private network; and

(h) A network intrusion prevention system to analyse network traffic to prevent known malicious activities from occurring within the Organisation's network.

5 At the time of the Incident, the work email accounts of the Organisation's employees were hosted on Microsoft Office 365 ("**Office 365**"),

and the Organisation's employees were able to access their work email accounts through the internet via a web-browser (i.e. web-mail). In June 2019, the Organisation implemented multi-factor authentication ("**MFA**") for all of its employees' work email accounts as part of its planned initiatives. The MFA implemented by the Organisation required its employees to key in a one-time password sent to their registered mobile number when accessing their work email accounts from a new device (the "**OTP Process**"). Upon successfully accessing their work email account on that device, employees had the option of choosing to "stay signed in" to their work email account on that authenticated device. Where this option was chosen, employees would not be required to undergo the OTP Process when subsequently accessing their work email accounts on that same authenticated device.

6 The Organisation represented that the above security solutions did not detect any anomalies and/or unusual activities in the Organisation's email traffic before 24 October 2019.

The Incident

7 On 24 October 2019, the Organisation's IT helpdesk received a complaint that one of the Email Accounts was not able to send outgoing emails. In conducting checks to address this complaint, the Organisation's IT helpdesk

discovered that Office 365 had automatically imposed restrictions on the Email Accounts. This is a security feature of Microsoft's Exchange Online Protection which indicated unauthorised access to the Email Accounts. Further investigations by the Organisation confirmed that the Email Accounts had been configured to automatically forward all incoming emails to the Third Party. This auto-forwarding of emails occurred between 8 March 2018 to 25 October 2019 for one of the Email Accounts, and between 1 April 2018 to 25 October 2019 for the other.

8 In total, 9,271 emails were forwarded from the Email Accounts to the Third Party. This resulted in the unintended disclosure of personal data belonging to 3,539 unique individuals, of which 1,923 unique individuals also had their Medical Information disclosed. The Affected Data Types were disclosed in different permutations and not all affected individuals had all of the Affected Data Types disclosed through the various forwarded emails.

9 For completeness, the MFA and OTP Process had been not implemented at the time when the Incident first occurred on 8 March 2018.

Remedial Measures

10 After discovering the Incident, the Organisation carried out the following remedial measures:

(a) Disabled the auto-forwarding feature for end-users;

(b) Increased the frequency of internal cybersecurity training and exercises;

(c) Implemented additional technical email and network security measures; and

(d) Refreshed and upgraded various of its existing network security measures.

11 The Organisation has advised that it will by 2022, upgrade, refresh and/or enhance its existing solutions for its:

(a) Network security measures; and

(b) Endpoint security measures.

Findings and Basis for Determination

12 In view of the circumstances of the Incident, the Commission's investigation focused on whether the Organisation had breached its obligation under section 24 of the PDPA 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 deciding what constitutes reasonable security arrangements and/or controls, organisations should take into consideration the nature of the personal data in question, as well as the impact that disclosure of that personal data might have on affected person(s). This is a fact-specific assessment that organisations should undertake when developing and/or implementing its security arrangements, policies, and controls. As stated in the Commission's Advisory on Key Concepts in the PDPA[1]:

> "*There is no 'one size fits all' solution for organisations to comply with the Protection Obligation*. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration *the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.* For example, in the employment context, it would be

[1] See sections 17.2 – 17.3 of Advisory Guidelines on Key Concepts in the PDPA (Rev 1 February 2021)

reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

In practice, an organisation should:

(a) *design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;*

(b) identify reliable and well-trained personnel responsible for ensuring information security;

(c) implement robust policies and procedures for *ensuring appropriate levels of security for personal data of varying levels of sensitivity*; and

(d) be prepared and able to respond to information security breaches promptly and effectively.

In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors may be considered:

(a) the size of the organisation and the amount and type of personal data it holds;

(b) *who within the organisation has access to the personal data;* and

(c) whether the personal data is or will be held or used by a third party on behalf of the organisation."

[emphasis added]

14 For the reasons set out below, it is determined that the Organisation failed to implement reasonable security arrangements to protect the personal data in the Email Accounts from the risk of unauthorised access and disclosure.

Failure to put in place reasonable security arrangements to meet its needs

15 Where the personal data in question is sensitive and/or may cause damage to affected individuals if compromised, organisations should implement stronger access and security measures. The Commission has issued guidance on this issue in its Guide to Securing Personal Data in Electronic Medium[2] (the "**Guide**") In particular, paragraphs 7.3 and 7.4 of the Guide state that:

[2] Guide to Securing Personal Data in Electronic Medium (revised Jan 2017)

> "7. 3. The strength of authentication, such as password requirements or other mechanisms for access to personal data, *should depend on the potential damage to the individual, such as potential damage to reputation or finances,* if such personal data is compromised…
>
> 7.4 More secure authentication methods include two-factor or multi-factor authentication. These involve the use of a combination of information that the user knows, such as a password or PIN, and an object that only the user possesses, such as a digital key, token or smart card, or a unique physical trait, such as the use of fingerprints in biometric technology. The use of multi-factor authentication increases confidence in the identity of the user accessing the system."
>
> [emphasis added]

16 The Commission's latest Guide to Data Protection Practices for ICT Systems[3] also recommends two tiers of (i) basic and (ii) enhanced data protection practices for organisations to adopt in different circumstances. The guidance remains that larger quantities and more sensitive personal data call for enhanced data protection practices:

[3] Guide to Data Protection Practices for ICT Systems (2021).

> "…For organisations that hold large quantities of different types of personal data or data that might be more sensitive to the individuals or organisations, they should additionally implement the relevant enhanced practices suggested.... The design and implementation of these protection measures should always take into consideration the extent of the sensitivity of the data based on the nature of business and types of services offered."[4]

17 In the present case, the Organisation ought to have implemented stronger security arrangements, policies and/or controls to manage its marketing department's Office 365 work email accounts, for the following reasons:

(a) The Organisation's marketing department routinely (on a daily basis) received and processed sensitive personal data, namely, the Medical Information of past, present and prospective patients.

(b) The volume of sensitive personal data processed by the Organisation's marketing department was not insignificant (1,923 individuals' Medical Information processed over 18 months).

(c) The marketing department's Office 365 work email accounts were accessible from the Internet (i.e. web-mail) which taken together

[4] Guide to Data Protection Practices for ICT Systems (2021), page 8.

with the above factors, exacerbated their vulnerability to unauthorised access.

18 Without prescribing the specific measures that would have been appropriate for the Organisation's circumstances, stronger security arrangements, policies and/or controls could have included:

(a) Implementing enhanced access controls for the marketing department's web-mail access (e.g. MFA, IP address based white-listing);

(b) Implementing policies and/or processes for the marketing department to collect Medical Information via a more secure platform (e.g. a separate web-portal);

(c) Implementing policies and/or processes for Medical Information to be regularly moved and purged from the marketing department's Office 365 email accounts, and stored in a more secure system (e.g. a non-Internet facing medical records or customer relationship management system); and/or

(d) Implementing policies and/or processes for Medical Information disclosed via the marketing department's email accounts to be better protected (e.g. password protecting email attachments).

19 For the avoidance of doubt, it is accepted that web-mail may be an appropriate and cost-effective way for organisations to provide their employees with out-of-office email access, and that it may not be necessary for organisations to implement enhanced controls to regulate the use of *all* types of web-mail accounts. It is incumbent on organisations to assess whether enhanced controls should be implemented to regulate the use of web-mail accounts, considering factors such as the volume and sensitivity of the personal data processed using such accounts.

20 In the present case, while MFA was eventually implemented for the marketing department's Office 365 work email accounts as an enhanced access control measure, this was unfortunately only after the Incident had occurred. Web-mail accounts are exposed to modes of attack that may defeat or circumvent 8-character alphanumeric password protection. Given that the marketing department was routinely processing personal data of a sensitive nature, it was incumbent on the Organisation to implement stronger security arrangements, policies and/or controls in conjunction with its adoption of web-mail.

21 In the premises, the Commission finds that the Organisation breached the Protection Obligation by failing to implement stronger security arrangements, policies and/or controls in respect of the Email Accounts.

Risks arising from Email Auto-Forwarding

22 The automatic forwarding of emails to external domains ("**Email Auto-Forwarding**") is a known security risk. In March 2018, it was reported that the Office of the Australian Information Commissioner was investigating a data breach incident notified by a member of the Maersk Group involving the auto-forwarding of 50,000 emails sent to 3 employees' accounts to external parties[5]. More recently, in a Private Industry Notification dated 25 November 2020, the United States of America's Federal Bureau of Investigations warned that cyber-criminals have been exploiting auto-forwarding rules on web-based email clients to perpetuate business email compromise scams and recommended, amongst other mitigation measures, that Email Auto-Forwarding be prohibited by default[6].

[5]https://www.zdnet.com/article/oaic-received-31-notifications-in-the-first-three-weeks-of-data-breach-scheme/
[6]https://www.ic3.gov/Media/News/2020/201204.pdf

23 Locally, in *Singapore Medical Association* [2020] SGPDPCS 13, an unauthorised user gained access to an email account and created an email rule to forward emails to an external email address. 137 emails were forwarded without authorisation, resulting in the unauthorised disclosure of the personal data of 68 individuals. The danger of allowing Email Auto Forwarding is clear, but there is an easy fix – organisations can simply disable this function and ensure that it remains disabled.

24 In the present case, the Organisation conducted a 'Business Impact Assessment' in 2013 on the use of Office 365 to assess the risks involved from the use of corporate email and instant messaging. The Organisation also subsequently conducted regular reviews and assessments of security risks arising from the use of Office 365 within the Organisation. Unfortunately, these steps did not include an assessment of the risks arising from Office 365's default setting which allowed Email Auto-Forwarding.

25 The Organisation, on its part, stated that it had not specifically examined disabling the default Email Auto-Forwarding feature in Office 365 because there had been no guidelines, standards, or benchmarks at the material time prior to the Incident recommending disabling of or management of risks from default Email Auto-Forwarding. Neither had it been a common industry practice to do

so prior to the Incident. In this regard, it is noted that Microsoft only released specific guidance on restricting or controlling Email Auto-Forwarding in Office 365 around July / August 2020[7].

26 It is recognised that Email Auto-Forwarding may be a useful function that serves valuable needs in relation to some email accounts. The Protection Obligation requires organisations, as part of their periodic security review, to assess the frequency and manner of use of Email Auto-Forwarding, and to weigh and counter the attendant risks. In particular, it is incumbent on organisations to apply their minds and make their own assessments of the risks and implications of adopting the default settings of "out-of-the-box" software solutions (see *COURTS (Singapore) Pte Ltd* [2020] SGPDPC 17 at [14] and *DS Human Resource Pte. Ltd.* [2019] SGPDPC 16 at [9]).

27 On balance, and on the facts of this case, the Organisation is given the benefit of the doubt that the lack of guidelines, standards or benchmarks at the material time may have affected its assessment of the risks arising from the

---

[7] See https://www.vansurksum.com/2020/08/25/microsoft-is-making-changes-related-to-automatic-email-forwarding-for-atp-customers-here-is-what-you-need-to-know/ referencing Microsoft's MC 218984 published July 2020 and MC220853 published August 2020. See also: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide

Office 365 default Email Auto-Forwarding rule. This omission will therefore not be factored in determining the enforcement action to be taken in this case. However, there must be no doubt that failure to make reasonable assessment of the risks from Email Auto-Forwarding within an organisation is breach of the Protection Obligation that would, in future cases, be met with the appropriate enforcement action.

The Commissioner's Preliminary Decision

28 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the factors listed at section 48J(6) of the PDPA were taken into account, as well as the following mitigating factors:

Mitigating Factors

(a) The Organisation took immediate remedial actions following the Incident;

(b) The Organisation cooperated fully with the Commission during the investigations;

(c) Prior to the Incident occurring, the Organisation had in place various technical security measures, including current market solutions; and

(d) The Organisation had conducted various data protection and cybersecurity training for its employees.

29 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 20 April 2022 and was invited to make representations on the same.

Representations Made by the Organisation

30 On 6 May 2022, the Organisation made the following representations to the Commission seeking a reduction in the amount of the financial penalty to be imposed:

(a) The Organisation had voluntarily notified the Commission and affected individuals of the Incident even though it was not legally obliged to do so under the PDPA, at the material time;

(b) There was no misuse of the affected personal data;

(c) The Organisation took prompt remedial actions to contain and mitigate the effects of the Incident, and prevent recurrence;

(d) The Incident was the Organisation's first breach of the PDPA; and

(e) The financial penalty which the Commissioner intended to impose was excessive in light of previous Commission decisions for similar or more serious breaches of the PDPA.

Representations on voluntary notification and lack of antecedents

31 The Organisation represented that it voluntary notified the Commission of the Incident despite not being legally obliged to do so, as the obligation for organisations to notify the Commission of notifiable data breaches (as defined under s 26B of the PDPA) only came into effect on 1 February 2022. The Organisation's voluntary notification of the Incident was taken into account when the Commission determined the preliminary financial penalty, and does not merit a further reduction of the same.

32 Likewise, the Organisation's representations that it had not committed any breaches of the PDPA prior to the Incident are not accepted. The Organisation's lack of antecedents had already been taken into account in calibrating the preliminary financial penalty.

Representations on the lack of misuse of the affected personal data

33 The Organisation represented that its private forensic expert had monitored the Internet and dark web from 25 February 2020 to 24 April 2020

and not found any information or data (including personal data of the affected individuals) relating to the Incident disclosed during that period. The Organisation further stated that it had not received any complaints from any affected individual as of the date of the representations in relation to misuse of their personal data. The Organisation therefore represented that no individuals had been harmed or had suffered loss as a result of the Incident.

34 In support of its representations, the Organisation cited the case of *Learnaholic Pte Ltd* [2019] SGPDPC 31 ("***Learnaholic***"), in which the Commissioner had taken into account the fact that "*while there was actual exfiltration of the Personal Data…there was no evidence of further exploitation, use or disclosure of the Personal Data by the attacker*."[8]

35 In the case of *Learnaholic* the main factors taken into account when deciding to reduce the preliminary financial penalty imposed were:

(a) A reduction in the total number of affected individuals due to a recalculation of figures; and

(b) The benefit of doubt given to Learnaholic as to the period of time the vulnerability in its system existed.

---

[8] *Learnaholic* at [34].

36 The lack of evidence of further exploitation, use or disclosure is not, *ipso facto*, a factor meriting a reduction of the financial penalty. The Organisation's representations are not accepted as the lack of an aggravating factor (i.e. subsequent exploitation, use or disclosure of personal data) is not in itself a mitigating factor.[9]

Representations on the prompt remedial actions taken by the Organisation

37 The Organisation represented that the Commission had not taken into consideration the immediate nature of the remedial action taken to contain the Incident, as well as the success of the immediate post-Incident remediation and recovery efforts. The Organisation further stated that it had not suffered any breaches of the same nature since the Incident, which was proof of the effectiveness of its remedial actions.

38 The Organisation's prompt remedial actions were already taken into account in determining the preliminary financial penalty. However, this is weighed against the lengthy time period during which the Email Auto-Forwarding took place (March 2018 – October 2019) and long delay in detecting the breach in the first place.

---

[9] See *Public Prosecutor v AOM* [2011] SGHC 29 at [37] and *Edwin s/o Suse Nathen v Public Prosecutor* [2013] SGHC 194 at [24] for the equivalent positions in the criminal sentencing domain.

Representations on previous Commission decisions

39 The Organisation cited two previous Commission decisions in support of its representations that the intended financial penalty was excessive for similar or more serious breaches of the PDPA. These two cases are *The National Kidney Foundation* [2021] SGPDPC 10 ("***NKF***") and *Singapore Medical Association* [2020] SGPDPCS 13 ("***SMA***").

NKF

40 The breach in *NKF* concerned a hacker who had gained access to the work email account of one of NKF's employees, thereby gaining access to 23,145 emails containing the personal data of approximately 500 individuals, including patients, employees, and third parties. The Organisation submitted that both cases were similar in the following areas:

(a) Types of personal data involved (i.e. sensitive medical information);

(b) Similar root causes and nature of the incidents;

(c) Failure by the organisations to implement 2FA/MFA for web-mail access at the time of the incidents;

(d) Increased data protection awareness as remedial measures; and

(e) Mitigating factors.

41 The Organisation distinguished *NKF* and submitted that a lower financial penalty was justified in this case for the following reasons:

(a) The Incident was less egregious than *NKF* because *NKF* involved:

(i) an additional category of sensitive personal data (bank account information), apart from just medical information; and

(ii) the hacker synchronising and downloading contents of the compromised email account; while no such synchronising or further use of the compromised email accounts was detected in the Incident;

(b) The Organisation had carried out far more substantial and comprehensive remedial measures than NKF; and

(c) The number of individuals affected by the Incident was not significantly higher than the number of individuals affected by the NKF incident.

42 The Organisation's representations are not accepted for the following reasons:

(a) In *NKF* only 8 patients' medical information was compromised, as opposed to the disclosure of 1,923 individuals' medical information

due to the Incident. The breach in the Incident was therefore of a much larger magnitude.

(b) The length of time that the breach went undetected was much longer in the Incident – the first email account was compromised in early 2018 and went undetected by the Organisation until October 2019, which was more than a year. This is much longer than the time it took for detection of the breach in *NKF*, where the hacker obtained access around 14 May 2020 and NKF discovered the breach on 17 May 2020.

(c) The number of individuals affected by the Incident is more than 7 times higher (500 in *NKF* as opposed to 3,539 in the Incident). The two incidents thus cannot be considered in the same bracket of egregiousness.

SMA

43 The breach in *SMA* concerned unauthorised access to an email account by brute force attack, and the subsequent forwarding of 137 emails containing the personal data of 68 individuals to an external email address. The Organisation submitted that both cases were similar in the following areas:

(a) Types of personal data involved; and

(b) Similar root causes and nature of the incidents.

44 The Organisation distinguished *SMA* and submitted that a lower financial penalty was justified because the Organisation had implemented more comprehensive security measures than SMA. In particular, the Organisation highlighted its own periodic changes of email account passwords and limit of the number of failed login attempts, in contrast with SMA which did not implement these measures.

45 The Organisation's representations are not accepted as the volume and sensitivity of personal data affected in the Incident was much higher than in *SMA*:

(a) The number of affected individuals in the Incident was 3,539; many times higher than the 68 affected individuals in *SMA*.

(b) The following categories of sensitive information were disclosed in the Incident but not in *SMA*: passport details, photographs, contact numbers, and notably, specific medical information. As a hospital, the Organisation must be held to a higher standard with regard to safeguarding medical information.

46 Notwithstanding the foregoing, the Commission notes that the Organisation voluntarily accepted the Commission's findings in the preliminary decision, that it had failed to comply with the Protection Obligation and

explicitly indicated what it would not seek to challenge these findings. The Organisation's voluntary acceptance of liability (even at this late stage) is accepted to have some mitigating weight, meriting a small reduction in the financial penalty. Had the Organisation accepted responsibility for the Incident at an earlier stage of the investigation, this may have merited a larger discount. An organisation that voluntarily accepts responsibility for its non-compliance with the PDPA is an organisation that demonstrates its commitment to the Accountability Obligation and shows that it can be responsible for the personal data in its possession or under its control.[10]

47 Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $58,000 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

[10] S 11(2) of the PDPA.

48 No further directions are necessary on account of the remedial measures already taken by the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION
