PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 18

Case Nos. DP-1802-B1719, DP-1802-B1744,
DP-1803-B1834, DP-1804-B1942, DP-1804-B1943

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

And

(1) Times Software Pte Ltd

(2) Dentons Rodyk & Davidson LLP

(3) Liberty Specialty Markets Singapore Pte Limited

(4) Red Hat Asia Pacific Pte Ltd

(5) TMF Singapore H Pte Ltd

… *Organisations*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements*

Data Protection *– Retention limitation obligation – Purpose for which the personal data was collected is no longer served by retaining data – Retention is no longer necessary for legal or business purposes*

Data Protection *– Data intermediary – Obligations of data intermediary and organisation which engages a data intermediary*

Times Software Pte Ltd & Ors

[2020] SGPDPC 18

Tan Kiat How, Commissioner — Case Nos. DP-1802-B1719, DP-1802-B1744, DP-1803-B1834, DP-1804-B1942, DP-1804-B1943

18 June 2020

Introduction

1 Times Software Pte Ltd ("**Times**") is an information technology services vendor that provides various services to its clients. Between January and February 2018, three organisations which directly or indirectly used Times' services became aware that the personal data of some their current and former employees (the "**Employee Data**") had been exposed online from Times' servers and could be found using the Google search engine (the "**Incident**"). These three organisations were Dentons Rodyk & Davidson LLP ("**Dentons**"), Red Hat Asia Pacific Pte Ltd ("**Red Hat**") and Liberty Specialty Markets Singapore Pte Limited ("**LIU**"). Each of these organisations submitted a data

breach notification to the Personal Data Protection Commission (the "**Commission**") after the Incident.

The Facts

The Relationship between the Parties and how Times had obtained the Employee Data

2 Dentons had, since 2001, engaged Times to use a payroll software application developed by Times (the "**Payroll Software**"). The Payroll Software was hosted internally on Dentons' servers. In or around November 2015, Dentons commissioned the development of a new functionality of the Payroll Software which would enable Dentons to create customised employee reports. Dentons provided their Employee Data to Times to test this functionality.

3 In December 2015 and February 2016, Red Hat and LIU respectively engaged TMF Singapore H Pte Ltd ("**TMF**"), a professional services company, for certain HR and payroll services. For this purpose, Red Hat and LIU provided TMF with their Employee Data.

4 In turn, TMF had, since 2008, engaged Times to use the Payroll Software to provide services to its clients, including Red Hat and LIU. The Payroll

Software was hosted on TMF's servers. Sometime between December 2015 and February 2016, TMF provided Times with Red Hat and LIU's Employee Data. The reason for doing so was disputed by TMF and Times:

(a) According to Times, TMF had provided the Employee Data for a one-time exercise which involved data migration and the development of a new functionality within the Payroll Software;

(b) In contrast, TMF asserted that the data migration and development of a new functionality within the Payroll Software were two separate and unconnected requests to Times. In this regard, TMF claimed that it had provided the Employee Data of Red Hat's and LIU's to Times only for the purposes of data migration, and was not aware of—and did not consent to—Times' use of the Employee Data to develop the functionality.

5 There was insufficient contemporaneous evidence to support either party's version of events. In particular, TMF and Times did not have a written agreement on the handing over of the Employee Data which could have provided more context. In any event, there is no need to make a finding on which version of events is to be believed. As explained further at [36] below, the findings regarding TMF's breach of its Protection Obligation under Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") are not dependent on

whether TMF had consented to Times' use of Red Hat's and LIU's Employee Data to develop the functionality within the Payroll Software.

The Disclosure of the Employee Data

6 The Employee Data handed over to Times by Dentons and TMF was stored in Times' File Server System ("**FSS**"). Between 21 December 2017 and 23 December 2017, Times suffered a hard disk failure in its FSS. To remediate this, Times restored a backup of the data in the FSS on or around 23 December 2017 and reset the FSS operating system settings to their default settings, which included disabling the password protection feature. As the FSS was accessible over the Internet, the Employee Data that was stored in the FSS was exposed to web crawlers and indexed by the Google search engine and stored in Google's cache.

7 In total, 616 employees had their Employee Data exposed over the Internet from 23 December 2017 to around mid-February 2018. This number comprised 400 employees from Dentons, 162 employees from Red Hat, and 54 employees from LIU. The types of Employee Data which was exposed during the Incident included:

(a) For Dentons: name, NRIC or other identification number, residential address, contact number, work designation, duration of employment and base salary;

(b) For Red Hat and LIU: name, NRIC or other identification number, date of birth, marital status, nationality, race, base salary, bank account information, income tax account number, addresses and mobile number.

8 Upon discovery of the Incident, the organisations took the following remedial actions:

(a) Times:

(i) Took action to take down all links to the Employee Data by contacting Google and other search engines (i.e., Bing and Archive.org);

(ii) Took all server hosting development files offline so that they were no longer available on the Internet and could only be accessed internally via Local Area Network with proper authentication;

(iii) Developed additional policies and SOP on data handling for its employees, which included the following requirements:

(A) Heads of departments are now required to conduct a weekly audit to ensure sensitive files are destroyed upon completion of work;

(B) Cross-department audits are to be done on a monthly basis, as well as upon completion of work;

(C) Random audits are to be done by the IT manager on a bi-monthly basis; and

(D) Servers published online will no longer accept unencrypted files.

(b) LIU:

(i) Imposed more stringent contractual provisions on TMF with regard to the services it is providing including dealing with data breaches or the protection of personal data;

(ii) Worked with Times to ensure that all relevant data, including the Employee Data, had been removed from Times' environments;

(iii) The Liberty Mutual Global IT Team undertook a comprehensive security review of TMF's services; and

(iv) Notified all its current employees of the Incident.

(c) Red Hat:

(i) Being the first party to discover the breach, notified Google to take down the Employee Data;

(ii) Notified all current employees and former employees of the Incident and offered free credit monitoring service to the affected employees; and

(iii) Obtained assurance from TMF and Times that Times had disabled the internal folder from public view, and that Times would perform audits to ensure all servers published on the internet that are meant for internal use were password-protected.

(d) Dentons:

(i) Notified its employees of the Incident; and

(ii) Obtained assurance from Times that all servers connected to the Internet were password protected.

(e) TMF:

(i) Ceased to allow Times to retain any of its clients' information for development purposes, and set up a UAT

environment for Times for future development of additional functionalities.

Findings and Basis for Determination

Breach by Times of Sections 24 and 25 of the PDPA

9 Times was a data intermediary[1] of Dentons as it processed personal data on behalf of, and for the purposes of Dentons. As explained further at [27] below, Times was also a data intermediary of TMF as it processed personal data on behalf of, and for the purposes of TMF, the relevant data here being Red Hat's and LIU's Employee Data.

10 A data intermediary is subject to both the Protection Obligation and the Retention Limitation Obligation under Section 24[2] and Section 25[3] of the PDPA. The Commission's investigations showed that Times had breached both these obligations.

[1] Section 2 of the PDPA defines "data intermediary".
[2] Section 24 of the PDPA requires organisations to protect personal data in their possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
[3] Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by the retention of the personal data, and retention is no longer necessary for legal or business purposes.

11 In relation to the Protection Obligation, Times had breached it in two ways. First, the processes in remediating the hard disk failure in its FSS fell short of the standard required under Section 24 of the PDPA. Times' Standard Operating Protocol ("**SOP**") required the employee who carried out the server restoration to enable the authentication function, i.e. password-protect function, so that only a user with proper credentials would be granted access to the data in the FSS. The employee's supervisor was also required to check that the authentication function was enabled. However, the relevant employee had failed to enable the authentication function after the server restoration. This was not discovered by the employee's supervisor as the supervisor did not take any measures to confirm that the authentication function was enabled.

12 It can be seen that even though Times had SOPs in place, the fact Times had not detected the employee's error in not enabling the authentication function shows that the security arrangement was not sufficiently reasonable. As set out in *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34 at [21], *"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*". Given the amount and type of personal data that Times was processing, Times should have ensured that their SOP included specific procedures that were designed to reasonably detect non-

compliance and to discourage deliberate, reckless or careless failures to adhere to the SOP by its employees.

13 Second, Times' other internal policies also fell short of reasonable protection expected for an organisation that handles the amount and type of personal data that Times handled:

(a) Times had poor password management policies in place. It was the prevailing practice of Times' employees to set the same password to the FSS prior to and after a server restoration. While this may be permissible for certain more routine restorations in the course of operational maintenance, organisations should set new passwords for server access control, especially where there has been a restoration of the server after security incidents;

(b) The Employee Data included bank account numbers and salaries. As the disclosure of such data may have a direct and significant impact on the individuals concerned, additional measures should have been adopted by Times to protect such data, for example, by encrypting such data, when storing such data in the FSS. This has been emphasised by the Commission in its Guide to Security Personal Data in Electronic Medium (Revised 20 January 2017); and

(c) Times should not have used live customer data for testing purposes. As highlighted in the Commission's Guide to Basic Data Anonymisation Techniques (Published 25 January 2018), using live personal data for testing involved risks as a development and/or test environment may be remotely accessed. Rather, Times should have used either anonymised or synthetic data, so that testing of the new functionality may be done without any risk to the personal data.[4]

14 As for Retention Limitation Obligation, Times admitted that the requested tool was implemented in December 2015 and the Employee Data of Red Hat's and LIU's Impacted Employee should have been deleted after that. In fact, Times' SOP on software development required employees to delete personal data once project sign-off has been obtained. However, in breach of the SOP, the employee who assisted in the development of the new functionality for the Payroll Software did not delete the personal data provided by TMF. No checks were conducted to ensure that the SOP was followed. Times had therefore contravened its Retention Limitation Obligation under Section 25 of the PDPA.

[4] [13] of Guide to Basic Data Anonymisation Techniques.

15 In the course of settling this decision, Times made representations proposing to take full responsibility for the Incident, and for a reduction in the quantum of financial penalty that the Commissioner had intended to impose. Times raised the following factors for consideration:

(a) The Incident was the first data breach in Times' 21 years of operations;

(b) No damages were reported as a result of the Incident;

(c) Times had improved their network security, conducted vulnerability assessments, and improved their SOPs to reduce human errors; and

(d) Their business had since been adversely affected by Covid-19.

16 Times' proposal to take full responsibility for the Incident does not absolve the other organisations that are also in breach. The PDPA imposes data protection obligations on all organisations in relation to personal data in their possession or control, and each organisation is individually responsible to comply with these obligations.

17 The other factors raised at [15(a)]-[15(d)] have were considered in mitigation. In particular, the exceptional challenges faced by businesses amid

the current Covid-19 pandemic have been taken into account, bearing in mind that financial penalties imposed should not be crushing or cause undue hardship on organisations.

18 All things considered, the financial penalty imposed on Times has been reduced to $20,000 for the contravention of the Protection Obligation and Retention Limitation Obligation of the PDPA. Although a lower financial penalty has been imposed in this case, this is exceptional and should not be taken as setting any precedent for future cases.

Breach by Dentons of Section 24 of the PDPA

19 Section 4(3) of the PDPA provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data was processed by the organisation itself. This means that both the organisation and data intermediary each have an obligation to make reasonable security arrangements to protect personal data that are in their possession or under their control. The Commission has in previous decisions stated that it is necessary for an organisation to put in place the appropriate contractual provisions with its data intermediaries to set out the obligations and responsibilities of the data intermediary to protect the

organisation's personal data, and the parties' respective roles to protect the personal data.[5]

20 In this case, it is not disputed that there was no written contract between Dentons and Times regarding the processing of the Employee Data by Times. Instead, Dentons represented that it had relied on a letter issued by Times in July 2014 (the "**Statement**") to protect personal data as evidence in writing of the contract. The salient terms of the Statement are reproduced below:

> "*As a Data Intermediary, Times Software Pte Ltd has always been committed in protecting your personal data and will implement the following standard operating procedures (SOP) to ensure that we are in full compliance with the new ruling:*
>
> a) *All employees of Times Software Pte Ltd ("staff") must get written consent from the customer before retrieving any personal data (such as company database or payroll related reports). The written consent must specify the identity and the purpose of usage by the applicant.*

[5] See for example *Re Cellar Door and Ors* [2016] SGPDPC 22 at [15]; *Re Singapore Telecommunications Limited* [2017] PDPC 4 at [14]; *Re Singapore Health Services Pte Ltd & Ors* [2019] SGPDPC 3 at [59].

b) *Staff should not reveal, distribute or broadcast any personal data that are deemed confidential by the client(s) even after resignation.*

c) *Printed copies of clients' confidential information or personal data are not to be recycled or reused. They must be immediately shredded upon completion of usage.*

d) *Staff are not allowed to keep or retain any customers' personal data upon completion of its intended purpose stated in the written consent.*

e) *Any electronic copies or duplications containing sensitive information, personal data or material which are to be sent or received by clients via any electronic medium* ***must*** *be encrypted with a password only known to the staff and the client. The password must not be in the same communicated e-mail or message. It should either be advised by phone conversation, sent in via Short Messaging Service (SMS) or in a separate mailer.*"

[emphasis in original]

21 In the course of settling this decision, Dentons raised the following factors in relation to the Statement for consideration:

(a) The Statement is a contract between Times and Dentons that is legally binding and fully enforceable. It contained three key commitments given by Times to Dentons: (i) the commitment to protect Denton's personal data and Times' full compliance with the PDPA; (ii) the commitment to not retain Denton's personal data upon completion of its intended purposes, and to shred such data upon completion of use; and (iii) the commitment to encrypt all electronic copies or duplications containing sensitive information or personal data which are to be sent or received by Dentons;

(b) The three commitments in the Statement mirror the obligations contained in the template clauses in the Commission's Guide on Data Protection Clauses for Agreements in relating to Processing of Personal Data (Published 20 July 2016);

(c) What is reasonable must be viewed in the context and the purposes for which personal data was being provided. Having regard to the scope and context of Denton's engagement with Times, any other

contractual obligations in addition to the Statement would be superfluous, and place an onerous and unreasonable burden on Dentons; and

(d) Lastly, where an adequate level of protection had been achieved in the circumstances (of the Statement), the Commission ought not to, with the benefit of hindsight, impose onerous additional requirements on Dentons for not meeting such enhanced requirements.

22 Dentons' representations that the Statement sufficed to discharge its Protection Obligation are not accepted as Dentons had overstated the effect of the Statement. While the Statement may meet the requirement of a contract evidenced in writing, it suffered from a significant flaw. The Statement omitted to cover the expected standard of protection for electronic *storage* of Employee Data. The commitments made by Times in the Statement pertained only to the conduct of staff, the security of *physical* copies of documents, and data protection (such as the need for encryption) *during electronic transmission*. Notably, the Statement did not specify any requirements for or include any commitments in relation to implementing security measures for the *electronic storage* of Employee Data, which was most relevant and paramount given that the Employee Data processed by Times was in electronic form and the Employee Data handed over by Dentons to Times was stored electronically in the FSS as mentioned at [6]. This was a serious omission of scope, which left

the standard of protection of a significant volume of electronic Employee Data unaccounted for.

23 The data protection commitments in the Statement were incomplete and could not reasonably be relied on by Dentons as a security arrangement to protect the Employee Data that was provided to Times.

24 Contrary to Dentons' representations, the requirement for an organisation to put in place contractual provisions to ensure its data intermediary will protect personal data is neither onerous nor unreasonable. In this regard, the Commission's Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data (Published 20 July 2016) sets outs sample clauses that an organisation may adapt to suit its needs. This is not an onerous process, and would not incur significant costs. In this case, the Statement that was introduced into the ongoing contractual relationship is sufficient written evidence of the data processing contract but it suffered from a significant defect in scope as explained at [22] above.

25 As for Dentons' representations that the Commission should not use the benefit of hindsight to impose additional requirements on organisations, the requirement for an organisation to ensure that its written contract with its data intermediary clearly specifies the data intermediary's obligation to protect

personal data is not new. As an illustration, that requirement was referred to in an earlier version of the Commission's Advisory Guidelines on Key Concepts in the PDPA (issued in September 2013), approximately two years before Dentons had provided its Employee Data to Times for processing.

26 For the above reasons, the finding that Dentons had contravened the Protection Obligation in failing to put in place the appropriate contractual provisions with Times for the protection of their Employee Data was maintained. After taking into account the relevant mitigating and aggravating factors listed at [44] below, it was decided that a warning to Dentons for the breach would suffice in this case.

Breach by TMF of Section 24 of the PDPA

27 TMF was a data intermediary of Red Hat and LIU as it was engaged to provide payroll services which involved the processing of Red Hat's and LIU's Employee Data. As a data intermediary, TMF was subject to the Protection Obligation set out at Section 24 of the PDPA and was required to put in place reasonable security arrangements to protect Red Hat's and LIU's Employee Data in its possession or under its control. What the "reasonable security arrangements" entail will depend on the context.

28 Based on the Commission's preliminary findings, it appeared that subsequent to its engagement as Red Hat's and LIU's data intermediary, TMF had outsourced to Times the processing of Red Hat's and LIU's Employee Data for payroll services. In this scenario, Times was not only a data intermediary of TMF, but may also be referred to as a "subsidiary data intermediary" of Red Hat and LIU.

29 To elaborate, the term "subsidiary data intermediary" may be used to describe an organisation who is a sub-contractor to a data intermediary, and who is sub-contracted to carry out data processing activities that are *directly related and necessary* to what the said data intermediary is supposed to undertake for an organisation (analogous to a data controller). As highlighted above, Times would be a "subsidiary data intermediary" of Red Hat and LIU if TMF had outsourced to Times the processing of Red Hat's and LIU's Employee Data for payroll services, because TMF was supposed to have performed these tasks in the contract TMF had with Red Hat and LIU.

30 Subsequently, TMF clarified in its representations to the Commission's preliminary findings that it did not sub-contract to Times any processing of Red Hat's and LIU's Employee Data for payroll services. Instead, it had provided Red Hat's and LIU's Employee Data to Times for the purposes of a one-time data migration exercise. As the data migration in this case was a different set of

processing activity unrelated to the payroll services that Red Hat and LIU had engaged TMF to provide, it would not be appropriate to refer to Times as a "subsidiary data intermediary" of Red Hat and LIU.

31 Although the term "subsidiary data intermediary" may be used to describe the position the sub-contractor is in vis-à-vis the data controller (ie, it is a "subsidiary data intermediary" of the data controller), the use of such a term is simply a convenient and informal label to describe such sub-contractors in the context of data processing where subcontracting is common. It has no legal implications; in particular, it does not mean that the data controller here is responsible for its subsidiary data intermediary in the same way as it does for its primary data intermediaries. This is because in many scenarios, the data controller may not even be aware that its primary data intermediary had engaged a sub-contractor, and hence it is in no position to influence its subsidiary data intermediary. Instead, in situations where there are multiple layers of sub-contracting and sub-processing of personal data, **there is a separate data controller and data intermediary relationship in each layer**. The scope of data processing outsourced in each layer of sub-contracting is determined by the relevant contract which should also set out the data controller's and data intermediary's respective obligations to protect the personal data. Therefore, even if Times was regarded as Red Hat's and LIU's "subsidiary data

intermediary" (not actually so in this case for the reason set out in the preceding paragraph), Red Hat and LIU would not be responsible for Times as if they were Times' data controller for the purposes of the PDPA. Times' data controller here would be TMF solely.

32 Indeed, TMF's role as Times' data controller and Red Hat's and LIU's data intermediary meant that TMF was subject to the Protection Obligation in putting in place "reasonable security arrangements", such as contractual mechanisms with Times, to ensure that Times had the necessary safeguards to protect the Employee Data.

33 In this regard, it is not disputed that there was no written contract between TMF and Times regarding the processing of the Employee Data. TMF was therefore found in breach of the Protection Obligation in the Preliminary Decision.

34 In the course of settling this decision, TMF made representations disputing the preliminary finding that it had breached the Protection Obligation, raising the following factors for consideration:

(a) TMF had conducted annual vendor assessments with Times, and Times had confirmed in those assessments that it had a formal data disposal policy in place, which had led TMF to incorrectly believe that

none of the Employee Data was retained by Times. In the circumstances, it would not be reasonable to expect TMF to conduct an invasive audit of Times' IT system to verify that the Employee Data was absent; and

(b) TMF did not ask Times to retain and use the Employee Data for the development of a new functionality within the Payroll Software. Times had done do without TMF's authorisation, and was not acting as TMF's data intermediary in doing so. Accordingly, TMF should not be held responsible for Times secret retention of the Employee Data.

35 While TMF's conduct of the annual vendor assessments is a mitigating factor that is taken into account, it does not suffice to discharge TMF's Protection Obligation. The annual vendor assessments would only assist to check that Times had not retained the Employee Data unnecessarily. However, it bears repeating here that TMF had not entered into any contract with Times with respect to Time's processing of Red Hat's and LIU's Employee Data on TMF's behalf. This means that the purpose and scope of the processing to be undertaken by Times, as well as Times' obligation to protect the relevant Employee Data, were not clearly set out in the first place.

36 On this note, the grounds for finding that TMF had breached the Protection Obligation is primarily due to TMF's failure to put in place the

necessary contractual provisions requiring Times to protect Red Hat's and LIU's Employee Data prior to the transmission of the data during the one-time data migration exercise. Hence, it is not necessary to make a finding on whether Times had used the Employee Data for the development of the new functionality tool. As mentioned at [4] above, TMF disputes this account and there was insufficient contemporaneous evidence to support either party's version of events.

37 Having carefully considered the facts of the case, the finding that TMF had contravened the Protection Obligation was maintained. After taking into account the relevant mitigating and aggravating factors listed at [44] below, it was determined that a warning to TMF for the breach would suffice in this case.

No Breach by Red Hat and LIU

38 For Red Hat and LIU, the question to be determined is whether they had taken "reasonable security arrangements" to protect their Employee Data when they provided the Employee Data to TMF for processing.

39 Red Hat and LIU had both entered into a written contract with TMF for the processing of their Employee Data. Both contracts were similarly worded and imposed a general obligation on TMF to comply with the "applicable law", with no express reference to compliance with the PDPA. Both Red Hat and LIU

were found to have contravened the Protection Obligation in the Preliminary Decision because in addition to an "applicable law" clause, they ought to have put in place more detailed contractual provisions setting out TMF's obligations to protect the Employee Data (which included bank account and salary information).

40 In the course of settling this decision, Red Hat made representations disputing the preliminary finding that it had breached the Protection Obligation, and raised the following factors for consideration:

(a) Although the contract between Red Hat and TMF imposed only a general obligation on TMF to comply with the "applicable law", there should be no ambiguity that the applicable data protection law is the PDPA given that both Red Hat and TMF are incorporated in Singapore; and

(b) The contract between Red Hat and TMF had to be read together with the Master Services Agreement ("**MSA**") between their parent companies. The MSA contained two pertinent clauses on data protection:

> "*TMF and its Affiliates shall use at least the same degree of care to protect the Confidential Information of Client and its Affiliations from unauthorised disclosure or access that TMF*

> *and its Affiliates use to protect its Confidential Information but not less than reasonable care*" (Clause 10.4 of the MSA); and
>
> "*[T]he processing and global transmission of Data shall comply with Applicable Law which includes among others the binding corporate rules of TMF on international data transfers*" (Clause 11.2 of the MSA).

41 The provisions in the MSA meant that TMF was contractually bound to protect the Employee Data of Red Hat with the same standard of care as its own data, and in any case, not less than reasonable care. TMF's internal data protection policies are therefore relevant in assessing the standard of protection that it was contractually required to put in place. In this regard, TMF's: (i) Personal Data Protection Policy; (ii) General Data Protection Regulation Statement; and (iii) Binding Corporate Rules for processing customer data set out comprehensive requirements on data protection.

42 The inclusion of such terms in the contracts between TMF and Red Hat are adequate to satisfy the "reasonable security arrangements" requirement in Section 24 of the PDPA. Accordingly, Red Hat had not contravened its obligations under Section 24 of the PDPA.

43 Similarly, the contract between LIU and TMF, read together with the MSA also incorporated TMF's Personal Data Protection Policy, General Data Protection Regulation statement and Binding Corporate Rules for processing customer data. For the same reasons set out at [40] and [41] above, it follows that the terms in the contracts between TMF and LIU are adequate to satisfy the "reasonable security arrangements" requirement in Section 24 of the PDPA. Accordingly, LIU had also not contravened its obligations under Section 24 of the PDPA.

The Commissioner's Directions

44 In determining the directions to be imposed on Times, Dentons, and TMF under Section 29 of the PDPA, the following factors were taken into account:

(a) In respect of Times:

Mitigating Factors

(i) It has implemented remedial actions to address the deficiencies that caused the Incident; and

(ii) It was cooperative in the course of investigation and had provided prompt responses to the Commission's requests for information; and

Aggravating Factor

(i) The Employee Data was of a sensitive nature, and should have warranted more careful processing.

(b) In respect of Dentons:

Mitigating Factors

(i) The Employee Data was provided to Times for a one-time transaction, and the processing by Times was not expected to be of an ongoing nature;

(ii) It had voluntarily reported the breach;

(iii) It had not directly caused the Incident;

(iv) It had implemented remedial actions to address the Incident; and

(v) It had fully cooperated with the Commission in its investigations and had provided prompt responses to the Commission's requests for information; and

Aggravating Factor

(i) The personal data which was subject to the Incident included bank account and/or salary information which ought to have been protected to a higher standard.

(c) In respect of TMF:

Mitigating Factors

(i) The Employee Data was provided to Times for a one-time transaction, and the processing by Times was not expected to be of an ongoing nature;

(ii) It had acted responsibly in conducting annual vendor assessments of Times;

(iii) It had not directly caused the Incident;

(iv) It had implemented remedial actions to address the Incident; and

(v) It was cooperative in the course of investigation and had provided prompt responses to the Commission's requests for information; and

Aggravating Factor

(i) The personal data which was subject to the Incident included bank account and salary information which ought to have been protected to a higher standard.

45 To summarise, the Commissioner directed:

(a) Times to pay a financial penalty of $20,000 within 30 days from the date of this direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full;

(b) A warning to be given to Dentons in lieu of a financial penalty; and

(c) A warning to be given to TMF in lieu of a financial penalty.

46 No further directions are necessary given the remediation measures already put in place by the organisations involved.