PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPC 3

Case No. DP-2210-C0378

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

And

Keppel Telecommunications & Transportation Ltd

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access and disclosure of personal data – Insufficient security arrangements – Failure to delete unnecessary personal data*

Keppel Telecommunications & Transportation Ltd

2024 SGPDPC 3

Lew Chuen Hong, Commissioner — Case No. DP-2210-C0378

14 May 2024

Introduction

1 On 21 October 2022 and 28 October 2022, the Personal Data Protection Commission (the "**Commission**") received notifications from Geodis Logistics Singapore Pte. Ltd. ("**GLS**") and Keppel Telecommunications & Transportation Ltd (the "**Organisation**") respectively about a data breach incident (the "**Incident**") involving unauthorised access and exfiltration of personal data from servers belonging to GLS. One of the affected servers (the "**Affected Server**") contained the personal data of, amongst others, the Organisation's employees, ex-employees, directors and shareholders (the "**Personal Data**").

2 Subsequently, the Commission commenced investigations to determine whether the circumstances relating to the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA**").

3 After carrying out preliminary investigations, on 27 February 2023, the Commission accepted a voluntary undertaking from GLS pursuant to section

48(L)(1)(a) of the PDPA for GLS to implement enhanced security arrangements. No further enforcement action was taken against GLS.

4 On 2 March 2023, the Organisation requested for the investigation to proceed under the Expedited Decision Procedure, which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision, and to the Organisation's breach of section 24 of the PDPA.

Facts of the Case

Relationship between Organisation and GLS

5 At the material time, the Organisation provided logistics and data centre services, with operations across Asia Pacific and Europe.

6 Prior to 1 July 2022, the Organisation was the sole shareholder of Keppel Logistics Pte Ltd (which is now known as GLS). On 1 July 2022, the Organisation divested then-Keppel Logistics Pte Ltd to Geodis International SAS, following which it was renamed to GLS (the "**Divestment**").

7 For ease of reference, "GLS" is used to refer to both Keppel Logistics Pte Ltd (prior to 1 July 2022) and Geodis Logistics Singapore Pte Ltd (from 1 July 2022 onwards).

Storing of Personal Data on Affected Server

8 At all material times, the Affected Server belonged to GLS. Prior to the Divestment, the Organisation and GLS utilised the Affected Server as a shared IT

resource. Personal data of, amongst others, the Organisation and its affiliated entities' employees, ex-employees, directors and shareholders was stored in the Affected Server.

Migration to Cloud in May 2020

9 In or around May 2020, the Organisation, then the sole shareholder of GLS, migrated its data (including the Personal Data stored on the Affected Server) (the "**Migration**") to an entirely cloud-based storage solution (the "**Cloud**"). The Migration was overseen by the Organisation's IT department, which provided guidance to other staff on the technical procedures for migrating their data to the Cloud. When briefing staff about the Migration in late 2018, the Organisation did not give specific instructions to delete the Personal Data from the Affected Server after the Migration. The actual data migration was not undertaken by the IT department because of IT access control restrictions, and was left to the relevant staff to carry out themselves. The data migration was also not supervised by the IT department because the staff were expected to be responsible for their own data and files.

10 In the circumstances, the Organisation's staff **did not delete** the Personal Data from the Affected Server after copying the said data to the Cloud. The Personal Data therefore continue to reside on the Affected Server post-Migration.

11 While the Organisation's prevailing policies and practices provided for the disposal / purging of data and decommissioning of systems that were no longer needed by the Organisation, the Affected Server continued being used by GLS for its day-to-day operations post-Migration. The Affected Server was therefore not

identified for decommissioning and the Personal Data contained therein was therefore not disposed / purged following the Migration. By the Organisation's own admission, it overlooked that the Personal Data continued to reside in the Affected Server post-Migration.

Divestment in July 2022

12 In the lead up to the Divestment in July 2022, the Organisation's IT department reminded staff in March 2022 to "*transfer*" files stored on the Affected Server to the Cloud, because the Organisation would not be able to access the Affected Server following the Divestment. However, it was again **not** made clear that the staff should also **delete** the files after the transfer. As with the Migration in May 2020, the Organisation **did not delete** the Personal Data from the Affected Server during the Divestment in July 2022. By the Organisation's own admission, at the point of Divestment, it had once again overlooked that the Personal Data continued to reside in the Affected Server.

The Incident

13 On or around 3 October 2022, the Organisation was alerted by a third-party cybersecurity consultant (engaged by a related entity of the Organisation) (the "**Consultant**") of suspicious activities in relation to the Affected Server.

14 Investigations revealed that an anonymous threat actor gained unauthorised access to the Affected Server on 5 September 2022 through a compromised account of one of GLS' vendors and accessed multiple files on the Affected Server between 1 and 2 October 2022.

15 There was also evidence of data exfiltration from the Affected Server. A ransomware group published nine encrypted files on the dark web which it claimed contained data from GLS, and one unencrypted file which it claimed was a list of the files contained within the nine encrypted files (the "**File Listing**"). The Organisation reviewed the File Listing and confirmed that it contained a subset of the files on the Affected Server. However, the Organisation was unable to ascertain whether the encrypted files in fact contained the Personal Data stored in the Affected Server.

16 While it is therefore not definitively known what data was actually exfiltrated, the Commission notes that the personal data of approximately 22,659[1] individuals ("**Affected Individuals**") was put at risk of unauthorised access and exfiltration, of which up to 7,184[2] individuals' personal data could have actually been exfiltrated.

17 The Affected Individuals comprised employees and ex-employees of the Organisation and its subsidiaries, the Organisation's shareholders when it was listed on the Singapore Exchange Securities Trading Limited (SGX-ST), and other individuals relating to the Organisation's finance departments or with whom the Organisation, its subsidiaries or their respective employees had commercial or business dealings.

18 In terms of the types of personal data affected for each individual:

(a) The majority of the datasets (up to 19,752) comprised a combination of the individual's name, address, number of shares, and any of the following: identity number, nationality, and country of origin.

[1] This is based on the Personal Data contained in the Affected Server.
[2] This is based on the File Listing.

(b) A smaller number of datasets (up to 2,907) included a combination of the individual's name and one or more of the following: address, identity number, full image copy of the identity document, passport, passport photo, email address, telephone number, signatures, bank account number, date of birth, salary, nationality, educational qualifications, family information and images and/or information on re-entry permit.

Partial notification of affected individuals

19 On 19 December 2022, the Organisation sought a waiver of the requirement to notify certain categories of overseas-based Affected Individuals[3] of the occurrence of the Incident under section 26D(7) of the PDPA, on the basis that the Organisation does not have contact information of these individuals and/or that the affected Personal Data is historical salary information and out-dated, such that the Incident is unlikely to result in significant harm.

20 Having considered the circumstances surrounding the Organisation's request, the Commission granted a waiver in respect of the individuals whose contact information the Organisation did not have and could not obtain after making reasonable enquiries.

21 However, the Commission refused to grant a waiver where the Organisation's sole reason for seeking the waiver was that the affected Personal Data concerned out-dated salary information as at 2018, because the Commission considered such

[3] In total, the Organisation sought a waiver of the notification requirement in respect of 140 individuals.

information to be sufficiently recent such that there is still a likelihood of significant harm accruing as a result of the unauthorised disclosure of their personal data.

22 Save for those individuals whom the Commission has waived the notification requirements for, the Organisation has notified all Affected Individuals whom it is required to notify under section 26(2) of the PDPA about the Incident.

Remedial actions

23 Following discovery of the Incident, the Organisation implemented the following remedial measures:

Actions to mitigate the effects of the Incident

(a) Worked with the Consultant to ensure that measures were implemented to contain and/or prevent the risk of further breach in relation to the Affected Server;

(b) Confirmed that GLS had disabled all accounts of the compromised GLS vendor and shut down the vendor's remote access to the Affected Server;

(c) Requested GLS to permanently purge all of the Personal Data from the Affected Server, which was done on 22 November 2022;

Actions to prevent recurrence of the Incident or similar incidents

(d) Reviewed the May 2020 migration plan to verify that all data in local storage had been deleted following the Migration;

(e) Conducted refresher training for all of the Organisation's staff to ensure user awareness and strict adherence to the Organisation's policies, procedures and processes; and

(f) Implemented a standard operating procedure for IT and cyber due diligence to address changes in ownership or possession and control of any IT assets.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation under section 24 of the PDPA

24 Based on the circumstances of the Incident as set out above, 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**").

25 In managing the risks of unauthorised access and/or disclosure, organisations must be mindful of its security arrangements relating to the deletion and disposal of personal data that is no longer necessary. Personal data that is no longer needed

and personal data contained in IT systems that are to be redeployed or sold should be properly disposed, e.g. by secure deletion or purging of such personal data[4].

26 Following the Migration of the Personal Data to the Cloud in May 2020, the Organisation should have ensured that the Personal Data had been deleted from the Affected Server. However, the Organisation failed to do so. Instead, the Organisation left the Migration to its staff without providing specific instructions to delete such data after the Migration and without providing sufficient supervision.

27 Thereafter, the Organisation had an opportunity to rectify the above failure during the Divestment in July 2022, but again failed to do so. Similar to the Migration exercise in May 2020, the Organisation again did not make clear during the Divestment that staff should delete data from the Affected Server, and failed to implement any measures to ensure that this had been done.

28 The Organisation has admitted that its:

(a) Failure to ensure the deletion of the Personal Data from the Affected Server post-Migration in May 2020; and

(b) Failure to ensure the deletion of the Personal Data from the Affected Server prior to the Divestment in July 2022,

[4]Pages 115 and 116 of the Commission's Advisory Guidelines on Key Concepts in the PDPA (https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act) and page 14 of the Commission's Guide to Data Protection Practices for ICT Systems (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Tech-Omnibus/Guide-to-Data-Protection-Practices-for-ICT-Systems.ashx?la=en).

constituted a breach of the Protection Obligation.

29 The Commission accordingly finds that the Organisation negligently breached the Protection Obligation by failing to ensure the deletion of the Personal Data from the Affected Server for a period of more than 2 years after the Migration.

Observations on other data protection practices

30 Separate to the above finding, the Commission observes that had the Organisation included the Personal Data stored on the Affected Server in its personal data asset inventory, this would have facilitated earlier identification and deletion of the Personal Data from the Affected Server. For the avoidance of doubt, these observations are made solely to provide guidance, and (i) do not constitute additional findings of breaches of the Protection Obligation by the Organisation in this case; or (ii) factor in any way in the Commission's final decision in this case.

31 The creation and maintenance of a personal data asset inventory is an established security practice. Amongst other things, it enables an organisation to track its personal data assets and ensures that its periodic security reviews cover all of its the personal data assets[5].

32 In the present case, the Organisation maintained an inventory of the data assets used for its business operations systems, which was reviewed periodically. However, this inventory did not include the Personal Data contained in the Affected Server. As such, despite its periodic reviews, the Organisation remained unaware

[5] ***Re Eatigo International Pte Ltd*** **[2022] SGPDPC 9** at [15] to [19], ***Re Management Corporation Strata Title Plan No. 3400*** **[2020] SGPDPC 10** at [13]

that the Personal Data continued to reside in the Affected Server for more than 2 years after the Migration, and therefore failed to take steps to ensure its deletion.

33 That said, it was not necessary for the Commission to make breach findings in relation to the above data protection practice in this case.

The Commissioner's Decision

34 In determining whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered.

35 The Commission recognises that:

(a) The Organisation took prompt actions after being alerted about the Incident to mitigate the effects of the Incident and to prevent a recurrence;

(b) Investigations were handled under the Expedited Decision Procedure, under which the Organisation admitted to the facts set out in this decision and to its contraventions of the Protection Obligation; and

(c) The Organisation was cooperative with the Commission's investigations.

36 However, in terms of the nature, gravity and duration of the non-compliance by the Organisation, the Organisation's breach of the Protection Obligation continued for a duration of **more than two years**. This long period of non-compliance, coupled

with the Organisation's failure to provide clear instructions and supervise its staff during the Migration and the Divestment processes, reveals systemic shortcomings in the Organisation's data protection processes.

37 The Commission notes that there were approximately 22,659 Affected Individuals, of which up to 7,184 individuals' personal data could have been exfiltrated.

38 The Commission further notes that some of the personal data affected included, amongst other things, specimen signatures, full images of identification cards and/or bank account numbers. This exposed certain individuals to greater risks of identity theft or actual financial losses.

39 Finally, for the purposes of assessing what amount of financial penalty would be effective to deter non-compliance with the PDPA, the Commission also took into consideration the turnover of the Organisation[6].

40 In quantifying the financial penalty to be imposed in any given case, the Commission aims to strike a careful balance between an amount that is (i) proportionate to the circumstances and effect of the organisation's non-compliance with the PDPA but (ii) that remains effective as a deterrent when considering the means of the organisation. In the present case, upon a consideration of all the factors listed under section 48J(6) of the PDPA, the Commission is of the view that a higher financial penalty is warranted to ensure that the financial penalty meted is

[6] See e.g. ***Re Fullerton Healthcare Group Pte Limited and Agape CP Holdings Pte Ltd*** **[2023] SGPDPC 5** at [39], ***Re Autobahn Rent A Car Pte Ltd*** **[2023] SGPDPCS 4** at [11], ***Re Century Evergreen Private Limited*** **[2023] SGPDPCS 5** at [11]

proportionate in light of the Organisation's long period of non-compliance with the Protection Obligation (including during the Migration exercise in May 2020 and again during the Divestment in July 2022) and the type and nature of the personal data affected. A higher financial penalty is also warranted to ensure that the financial penalty meted will be effective in ensuring future compliance with the PDPA and to achieve the requisite deterrent effect.

41 Based on the above, the Commission determined that the Organisation should pay a financial penalty of $120,000 within 30 days from the date of the 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.

42 In view of the remedial actions already been taken by the Organisation, no further directions need be issued to the Organisation.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION