PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCR 1

Case No DP-2007-B6670

In the matter of a reconsideration application under section 48N(2)
of the Personal Data Protection Act 2012

And

Terra Systems Pte. Ltd.
… *Organisation*

RECONSIDERATION DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Unauthorised modification of personal data – Insufficient security arrangements – Failure to implement reasonable access controls – Failure to implement written policy*

Data Protection *– Protection obligation – Sensitivity of personal data*

Terra Systems Pte. Ltd.

[2022] SGPDPCR 1

Lew Chuen Hong, Commissioner — Case No. DP-2007-B6670

4 March 2022

[Editorial note: This was an application for reconsideration of the decision in Terra Systems Pte. Ltd. [2021] SGPDPC 7.]

Background and Application for Reconsideration

1 In *Terra Systems Pte. Ltd.* [2021] SGPDPC 7 (the "**Decision**"), Terra Systems Pte. Ltd. (the "**Organisation**") was found to be in breach of the Protection Obligation in section 24 of the Personal Data Protection Act 2012 (the "**PDPA**"). The grounds of decision and the full facts of the case are set out in the Decision.

2 In summary, the Organisation had been awarded a government contract to provide call centre services ("**Call Centre**") to help verify the whereabouts of persons serving "Stay-Home Notices" ("**SHNs**"). For its internal administration of the Call Centre, the Organisation created a customer relationship management portal ("**Portal**"). The Portal contained personal data of persons serving SHNs which was received from the Immigration and Checkpoints Authority, including each person's name, last 4 digits of NRIC, gender, contact number, last day of SHN,

address where SHN was served and COVID-19 Test Appointment dates (collectively, the "**SHN Data**").

3 The Portal was designed to be accessible by the Organisation's employees from home via the Internet, and the Organisation's employees were granted different levels of access to the Portal depending on their respective roles:

(a) Directors and managers were assigned unique user IDs and passwords to log into the Portal, and were able to view all cases in the Portal.

(b) Team leaders were also assigned unique user IDs and passwords to log into the Portal, and were able to view all cases assigned to agents in their teams.

(c) Agents were temporary staff employed to contact the persons serving SHNs. They were able to view only the cases assigned to them and would type in remarks in a specific "remarks" column after a case had been attended to. Agents were assigned simple user IDs based on their respective teams (e.g. the user ID "D03" referred to agent number 3 in team D). Agents use their user IDs and the common daily password to log into the Portal. The common daily password was shared with them during a daily morning Zoom briefing by the Organisation's management.

4 On 14 July 2020 and 21 July 2020, the Portal was accessed and modified without the Organisation's authorisation (the "**Incident**"). In particular, crude remarks had been inserted in the remarks field of 3 cases in the Portal on 14 July 2020, and a crude comment had been inserted in the remarks field of another case assigned on 21 July 2020.

5 The perpetrator is believed to be an ex-employee of the Organisation who accessed the Portal on two occasions:

(a) On 14 July 2020, the perpetrator is believed to have obtained the login details for the morning Zoom briefing from other employees, and accessed the Portal after finding out the daily common password for the Portal at the morning Zoom briefing.

(b) On 21 July 2020, the perpetrator is believed to have directly obtained the daily common password from another employee who was unaware that his employment had been terminated.

6 The Organisation was found to have contravened the Protection Obligation on the following basis, and directed to pay a financial penalty of $12,000:

(a) The Organisation had failed to implement reasonable IT access controls to the SHN Data in the Portal, by adopting (i) generic user IDs for agents which were known to all or guessable, and (ii) a daily common password for all agents; and

(b) The Organisation had failed to implement adequate policies to mitigate the risks created by the use of a daily common password to access the Portal.

7 On 3 September 2021, the Organisation submitted an application challenging the Decision (the "**Application**"). In the Application, the Organisation disputed the finding of breach of the Protection Obligation. In the alternative, the Organisation asked for the financial penalty to be waived and for a conditional warning to be administered instead.

Nature of the Application

8 The Application was stated to be pursuant to section 48N (relating to applications for reconsideration of directions or decisions) and section 48Q (relating to appeals from the Commission's direction or decision to the Chairman of the Appeal Panel) of the PDPA. The Application was treated as a reconsideration application, instead of as an appeal for two reasons. First, pursuant to section 48Q(3) of the PDPA, "[w]here an application for reconsideration has been made under section 48N, every appeal in respect of the same direction or decision which is the subject of the application for reconsideration is deemed to be withdrawn". Accordingly, any appeal by the Organisation in respect of the Decision is deemed to have been withdrawn. Additionally, the Application was submitted to the Commission and not to the Chairman of the Appeal Panel. This evinced a subjective intention to invoke the reconsideration procedure.

The Organisation's Submissions

9 The submissions raised by the Organisation can be summarised in three main areas. First, the Organisation claimed that neither the PDPA nor the government contract awarded to it prescribed the degree or scope of IT access controls to the SHN Data. Nevertheless, the Organisation claimed that it had implemented reasonable IT access controls by renewing the agents' passwords on a daily basis, and only providing the passwords to the agents on a need-to-know basis. Additionally, the Organisation had implemented policies to mitigate the risks from using a common password to access the Portal:

(a) The daily common password was only informed to agents reporting to work in the morning over a common Zoom call;

(b) Access to the morning Zoom call in turn required another password that was provided to agents every morning;

(c) The Organisation had verbally informed all agents during the morning Zoom call that passwords shall not be shared or disseminated, and agents had been informed to look for their team leaders if they forget the said password;

(d) The Organisation had taken efforts to ensure that the SHN Data was purged from the system daily; and

(e) The Organisation had taken additional effort to have each new agent who worked on the Call Centre sign confidentiality agreements and undertakings to safeguard official information, and abide by a Data Protection Policy for Employees and Job Applicants.

10 Second, the Organisation submitted that the alleged perpetrator of the Incident had been authorised to access the SHN Data at the material time, as he was effectively still an employee of the Organisation and needed such access for his functions. Taking reference from *Bellingham v Reed* [2021] SGHC 125 ("***Bellingham***"), the Organisation argued that the alleged perpetrator of the Incident had misused information outside the functions of his employment. Hence, the alleged perpetrator had acted in his own personal accord, and his act did not have a close connection to his employment with the Organisation such that the Organisation should

not be held responsible for those actions, taking reference from the United Kingdom Supreme Court's decision in *WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondent)* [2020] UKSC 12 ("***WM Morrison***").

11 Third, the Organisation cited the Commission's previous decisions in *Water + Plants Lab Pte Ltd* [2020] SGPDPC 22, *Flying Cape Pte Ltd and another* [2021] SGPDPCS 4, *St Joseph's Institution International Ltd* [2021] SGPDPCS 2, *Chapel of Christ the Redeemer* [2021] SGPDPCS 1, *Everlast Projects Pte Ltd and others* [2020] SGPDPC 20, *R.I.S.E Aerospace Pte Ltd* [2020] SGPDPC 21 and *Chan Brothers Travel Pte Ltd* [2020] SGPDPC 11, and stated that these decisions had involved more serious contraventions of the PDPA but that no financial penalties had been levied. In contrast, only 4 individuals' personal data was affected in the Incident, the personal data affected was not sensitive, there was no exfiltration or public exposure of the SHN Data, prompt remedial measures had been implemented with no loss of personal data, the Organisation had voluntarily reported the Incident to the authorities, and the Incident was caused by an employee going rogue with the data and no reasonable amount of safeguarding could have prevented the Incident. On the sensitivity of the personal data affected, the Organisation disagreed that the SHN Data was sensitive in nature, and pointed to several social media posts where different individuals had shared about their SHN experiences publicly.

Findings and Basis for Determination

Sufficiency of the Organisation's security arrangements

12 As a data intermediary, the Organisation is subject to the Protection Obligation. It must implement security arrangements to prevent unauthorised access to or modification of the SHN Data that is in its possession or under its control. Even if the government contract did not specifically prescribe how the SHN Data was to be protected, this does not exempt the Organisation from its Protection Obligation. It has to implement reasonable security arrangements to protect the SHN Data which was in its possession. In fact, the Organisation's implementation of roles-based access / different levels of access to the Portal for its employees (see [3] above) shows that the Organisation did in fact recognise the need to differentiate the levels of access granted to different employees, in order to protect the SHN Data. The question

is therefore whether the security arrangements were sufficient to enable the Organisation to discharge its Protection Obligation.

13 As stated in the Commission's Advisory Guidelines on Key Concepts in the PDPA (revised 1 October 2021) at [17.2], there is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Instead, it is for each organisation to assess the risks in the context of the sensitivity and volume of the personal data in its possession or control and implement reasonable measures to address these risks.

14 Context is important. The Organisation was engaged to establish the Portal to assist in the management of persons under SHN, during the initial phase of the global COVID-19 pandemic. The Organisation was part of the national effort in managing a public health crisis during a time when there was significant and widespread public concern. The Incident occurred soon after the end of the nationwide circuit breaker period, during which time only essential business activities could take place and the vast majority of residents were required to remain at home. Equally important is the nature of the personal data that they were managing. SHN Data meant that these persons had been in close contact with affected individuals. At that stage of the pandemic, such data had to be handled with much higher levels of care.

15 In this context, the Organisation's access controls and policies were inadequate. The Organisation had used generic user IDs for their agents which were known to all or easily guessable (e.g. "D03" for agent number 3 in team D). While the Organisation had changed the common password to access the Portal every day and only informed the agents reporting to work in the morning of the new common password using Zoom, the password to access the Portal remained a common one shared amongst all agents. This meant that anyone familiar with the number of teams and average team size would be able to easily guess another agent's user ID, and thereafter access another agent's cases on the Portal using the common password. Even though the SHN Data was purged from the Portal daily, prior to being purged, the SHN Data remained exposed to significant security risks.

16 The Organisation had also identified the risk that the daily common password was easily shared. The risks associated with use of a common password were exacerbated by the fact that the Organisation's agents were temporary staff and personnel changes were to be

expected. The Organisation therefore verbally informed all agents that passwords shall not be shared and to look for their team leaders if they forgot the said password. However, verbal reminders are not enough. As stated in *Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 at [18], informal practices and verbal reminders were an insufficient security arrangement for purposes of compliance with the Protection Obligation. Written policies are required to ensure that all agents are aware of their responsibilities and know what they need to do. It is not enough to just rely on general confidentiality and official secrets undertakings that agents had to sign before they commenced work at the Call Centre. As stated in the Decision at [19], the Organisation should have implemented written policies (1) to prohibit agents from disseminating or sharing the daily common password (including the password for the daily Zoom meetings at which the daily common password was shared), and (2) to require any agents to obtain the daily common passwords directly from their team leaders or managers, who would be better placed to verify the requestor's employment status.

17 Accordingly, the IT access controls and policies implemented by the Organisation did not constitute reasonable security measures as required under the Protection Obligation.

Whether the alleged perpetrator had been authorised to access SHN Data at the time of the Incident

18 The Organisation submitted that the alleged perpetrator of the Incident was authorised to access the SHN Data at the time of the Incident, as he was effectively still an employee of the Organisation and needed such access for his work functions (see [10] above). However, this is inconsistent with both the Organisation's practice and also its intention, and therefore cannot be accepted:

(a) The Organisation did not authorise all agents to access the SHN Data daily. Instead, only agents who reported to work in the morning were authorised to access the SHN Data, and even then, such access was limited to the cases assigned to them for that day. Agents were also only able to view the cases assigned to them on the Portal, and were <u>not</u> authorised to access cases assigned to other agents (see [3(c)] above).

(b) More importantly, the alleged perpetrator had been placed on garden leave at the time of the 1st incident on 14 July 2020, and his employment had been terminated

by the Organisation by the time of the 2nd incident on 21 July 2020. The alleged perpetrator was not assigned any cases, and therefore no longer authorised to access any of the SHN Data on both dates of the Incident. Needless to say, the alleged perpetrator was not authorised to modify any cases.

19 The Organisation relied on *Bellingham* and *WM Morrison* to submit that the alleged perpetrator of the Incident had misused information outside the functions of his employment and that the Organisation should not be held responsible for those actions (see [10] above). *Bellingham* and *WM Morrison* do not assist the Organisation's case:

(a) *Bellingham* was concerned with a private action under the then-section 32 of the PDPA where Reed's former employer sued Reed for using customer data obtained during the former employment. Reed's new employer was not a party in the suit. The case therefore does not address whether Reed's new employer ought to be vicariously liable for Reed's actions.

(b) Meanwhile, *WM Morrison* concerns the circumstances in which an employer was held vicariously liable under the UK Data Protection Act 1998 for its employee's breaches of duties imposed by that Act.

20 Crucially, the Organisation's contravention of the Protection Obligation is premised on its own failure to implement reasonable security arrangements to protect the SHN Data from the risk of unauthorised access. The Organisation's liability is not based on vicarious liability for the alleged perpetrator's actions.

Organisation's reliance on Commission's previous decisions

21 The Organisation relied on the Commission's previous decisions to submit that no financial penalty had been levied for more serious contraventions of the PDPA (see [11] above), and this submission was substantively similar to representations made by the Organisation to the Commission prior to the finalisation of the Decision. These claims were considered and rejected in the Decision, and are also rejected in this Application.

22 As stated in the Decision, every case is decided based on an evaluation of *all* the relevant facts and circumstances, and in a manner that is fair and appropriate for the particular organisation investigated. It bears repeating that context is important, and the context of this case makes it necessary to impose a financial penalty. The Organisation was part of the national effort in managing a public health crisis during a time when there was significant and widespread public concern. The Incident occurred soon after the end of the circuit breaker period, during which time only essential business activities could take place and the vast majority residents were required to remain at home. The nature of the SHN Data meant that the Organisation was managing data that these persons had been in close contact with affected individuals. At that stage of the pandemic, such data had to be handled with much higher levels of care.

23 In particular, the following facts of the present case justify a financial penalty levied on the Organisation:

Number of affected individuals:

(a) It is not accurate for the Organisation to submit that the personal data of only 4 individuals was affected in the Incident. As stated in the Decision, while only 4 records had been modified, the SHN Data of 125 individuals had been at risk of exposure in the Incident.

Type and nature / sensitivity of personal data involved:

(b) The present case involved SHN Data, which needed to be handled much more carefully given the time of the Incident within the larger public health context. The Organisation's submission that the SHN Data was not sensitive in nature (see [11] above), had been raised in representations to the Commission prior to the finalisation of the Decision. This premise was rejected in the Decision, and is rejected in this Application as well.

(c) As mentioned in the Decision, the SHN Data denoted the risk of a person's exposure to the COVID-19 virus. The sensitivity of the SHN Data is underscored by (1) the uncertainties surrounding COVID-19, a very transmissible virus, at the time of the Incident, (2) the high public concern at the time of the Incident in the earlier days

of a national health emergency, and (3) the fact that persons on SHN were pending COVID-19 test results and had not yet tested negative for COVID-19, which would add to the stigma for such persons (i.e. as opposed to persons who had already completed their SHN and not tested positive).

(d) The need to protect SHN Data is not simply based on hypothetical effects. On the contrary, events have demonstrated the very real consequences of actual or perceived exposure to the COVID-19 virus, such as the discrimination against employees of healthcare institutions that were the hotbed of COVID-19 transmissions, and businesses denying services to customers whose TraceTogether App reflected a "potentially exposed" status.[1]

(e) While a few individuals may have chosen to voluntarily share their personal data in a personal or domestic capacity on social media, this does not dilute the obligations of organisations under the PDPA to process sensitive data with adequate safeguards.

Nature of non-compliance with PDPA:

(f) The Incident occurred because the Organisation failed to implement proper IT access controls. It used commonly known or guessable user IDs and a common password for over 50 users, which was shared on a common platform. The Organisation also failed to implement policies to mitigate the associated risks. The Organisation had a relatively higher level of culpability in the Incident, within the context of a national health emergency, as it employed very poor access control measures that were easily circumvented. The extent of the Organisation's negligence within the context of a national health emergency, justified the imposition of a financial penalty in its case.

Modification of personal data:

[1] *See* Channel News Asia, "*Discrimination of healthcare workers due to coronavirus 'disgraceful': Amrin Amin*" dated 12 February 2020 (accessible at https://www.channelnewsasia.com/singapore/wuhan-virus-coronavirus-covid19-discrimination-healthcare-worker-776736); Straits Times, "*Students of driving school turned away as TraceTogether records show close proximity to Covid-19 cases*" dated 7 May 2021 (accessible at https://www.straitstimes.com/singapore/driving-students-turned-away-as-their-tracetogether-records-indicate-close-proximity-with) and Straits Times, "*TTSH healthcare workers refused by cab drivers, turned away by some hotels*" dated 18 May 2021 (accessible at https://www.straitstimes.com/singapore/ttsh-healthcare-workers-refused-by-cab-drivers-turned-away-by-some-hotels).

(g) The Incident involved both the access to and modification of personal data.

24 While the Organisation contended that the Incident was caused by an employee going rogue and that no reasonable amount of safeguarding could have prevented the Incident, this is not accepted. As stated at [20] above, the Organisation's contravention of the Protection Obligation is premised on its own failure to implement reasonable security arrangements to protect the SHN Data from the risk of unauthorised access and modification.

25 In calibrating the quantum of the financial penalty imposed, the Commission had taken into account the factors raised by the Organisation, such as the fact that the Incident only affected a limited number of persons, the Organisation's voluntary reporting, the prompt implementation of remedial measures, and that there was no material financial impact arising from the Incident.

26 Having carefully considered the Application, and taking into account all the relevant facts and circumstances, the Commissioner maintains the finding of the Organisation's contravention of the PDPA and the financial penalty of $12,000 imposed.

Conclusion

27 Given the foregoing, the Commissioner hereby affirms the Decision as follows: The Organisation is required to pay a financial penalty of $12,000 within 30 days from the date of this Reconsideration 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.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION