DECISION OF THE
PERSONAL DATA PROTECTION COMMISSION

Case Number: DP- 1409-A099

(1) THE CELLAR DOOR PTE LTD (UEN No. 200001784C)
(2) GLOBAL INTERACTIVE WORKS PTE. LTD. (UEN No. 200822173M)

... Respondents

Decision Citation: [2016] SGPDPC 22

GROUNDS OF DECISION

23 December 2016

A. BACKGROUND

1. On or around September 2014, the Personal Data Protection Commission ("**Commission**") found unauthorised postings on a website (http://pastebin.com/jiQw38nU) known as "Pastebin", comprising of personal data of customers and users (collectively, the "**customers**") of The Cellar Door Pte Ltd's ("**Cellar Door**") website of Cellar Door, which was made available online.

2. The Commission undertook an investigation into the matter and its findings and grounds of decision are set out below.

B. MATERIAL FACTS AND DOCUMENTS

3. Cellar Door is in the business of selling food and wine products, and has a business website with the address of http://www.thecellardoor.com.sg (the "**Site**").

4. The Site was developed by a company known as Global Interactive Works Pte. Ltd. ("**GIW**"), which specialises, amongst other things, in website design, development and hosting. GIW was engaged to design and develop the Site. The Site and Cellar Door's customer database were hosted on GIW's server. As part of these services, GIW would also backup the Site and customer database. Only GIW's staff would have access to these backups.

5. The disclosure of personal data on Pastebin comprised of the full names, mobile and residential telephone numbers, residential addresses, email addresses and passwords of Cellar Door's customers. The data that was disclosed on the Pastebin website was a subset of Cellar Door's entire customer database. Cellar

Door was not aware of the unauthorised disclosure on the Pastebin website prior to the Commission informing Cellar Door of the said disclosure.

6. In response to the Commission's inquiry into the matter, GIW stated that its engineers were unable to determine the reasons for the disclosure of the personal data of Cellar Door's customers on the Pastebin website. GIW developed the Site for Cellar Door in 2011. Subsequent to that, Cellar Door engaged GIW to host the Site and Cellar Door's customer database, but it did not sign up for a maintenance package to maintain its Site and customer database.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Issues for determination

7. The issues to be determined in the present case are as follows:

   (a) Whether GIW was acting as a data intermediary for Cellar Door in relation to the personal data hosted on GIW's servers.

   (b) If GIW is a data intermediary for Cellar Door, what were the respective obligations of GIW and Cellar Door under the Personal Data Protection Act 2012 (the "**PDPA**").

   (c) Whether Cellar Door and GIW had complied with their obligations under Section 24 of the PDPA.

Relevant Provisions

8. Section 24 of the PDPA provides that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

9. Section 4(2) of the PDPA confers an obligation on the data intermediary to comply with the Protection Obligation and the obligation to cease to retain personal data under Sections 24 and 25 of the PDPA respectively.

10. Further, Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Issue A: Whether GIW is a data intermediary for Cellar Door

11. GIW was engaged by Cellar Door to host the Site and customer database on its servers. The set of operations that GIW would carry out in furtherance of this engagement, such as the storage or holding of personal data on GIW's servers, or the organisation or management of personal data in the customer databases,

would fall squarely within the definition of “processing” under Section 2(1) of the PDPA. As such, GIW was processing the personal data of Cellar Door’s customers.

12. As GIW carried out the abovementioned operations on behalf of Cellar Door and for its business purposes, GIW comes under the definition of a “data intermediary” under the PDPA, and is therefore required to comply with the Protection Obligation.

Issue B: Cellar Door and GIW respective obligations under the PDPA

13. Having determined that GIW is a data intermediary for Cellar Door, it is appropriate for the Commission to elaborate on the respective obligations of Cellar Door and its data intermediary, GIW, under Section 24 of the PDPA in respect of the personal data in question.

14. Pursuant to Sections 4(2) and 4(3) of the PDPA, both Cellar Door and GIW are obliged under Section 24 of the PDPA to ensure that there are reasonable security arrangements to protect the personal data of Cellar Door’s customers.

15. In the Commission’s view, Cellar Door has the primary responsibility of ensuring the overall protection of the personal data, and it was for Cellar Door to put in place the necessary security measures to protect the personal data. Cellar Door is not discharged of its responsibility simply because it had engaged a data intermediary (ie GIW) to provide hosting and database services for Cellar Door. It is incumbent on Cellar Door to take the necessary steps to ensure the overall protection of data, even though it may have engaged GIW to assist with certain data operations. For example, Cellar Door may put in place contractual arrangements which clearly define the scope of GIW’s responsibilities, and follow through with operational procedures and checks to ensure that GIW carries out its functions.

16. GIW, on the other hand, has the direct responsibility of ensuring the protection of the personal data, as it was hosting the personal data on its servers, and was the site administrator for the Site and customer database. GIW would therefore also need to ensure that reasonable security arrangements are put in place to protect the personal data in its possession or under its control. The extent of GIW’s obligations are scoped in accordance with the contractual arrangement it had with Cellar Door. In this case, it is the protection of customer database hosted by it.

17. A secondary issue in this case would be the distinction between possession and control of personal data. The Commission is of the view that it is possible for the same dataset of personal data to be in the possession of one organisation, and under the control of another. For example, in a situation where the organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data set while, simultaneously, the data intermediary may have possession of the same personal data set.

18. In the present case, the Commission finds that the personal data handled by GIW was still under the control of Cellar Door, given that GIW was Cellar Door's service provider, and the personal data that GIW had processed (as defined in the PDPA, and examined at paragraphs 11 and 12 above), were for Cellar Door's business purposes.

19. Accordingly, even though Cellar Door was not in direct possession of the personal data that was held in GIW's servers, it was still obliged to protect the data by operation of Section 4(2) of the PDPA (as mentioned at paragraph 14 above), and, additionally, by the fact that it had control over the personal data (as found at paragraph 18 above).

20. The Commission now turns to its assessment of whether Cellar Door and GIW have complied with their obligation under Section 24 of the PDPA respectively.

Issue C: Whether Cellar Door and GIW have complied with their obligations under Section 24 of the PDPA

21. From its investigations, the Commission has found that there was a lack of adequate security arrangements in place to protect the personal data in question pursuant to Section 24 of the PDPA. Broadly, it was found that Cellar Door and GIW had (1) inadequate security policies and processes to protect the personal data; and (2) failed to put in place an overall security to guard against intrusions, attacks or unauthorised access.

(1) Inadequate security policies and processes

22. Having in place adequate security policies and processes is the cornerstone for protecting personal data in the IT setting. In the Commission's view, an adequate security policy should be based on the organisation's assessment of the risks, vulnerabilities and threats facing the IT system and its determination of what the system needs to address these risks, vulnerabilities and threats. In turn, the processes of the organisation can be built upon the security policy that the organisation had put in place. This ensures oversight; proper accountability of the personal data; and control over the measures and processes protecting the personal data.

23. Without such a security policy in place, an organisation may not, amongst other things, be able to detect that a data breach has happened; may not be able to determine what went wrong; and may not know what are the corrective measures to be taken. This was what has happened in this case.

24. In the Commission's view, the organisation, and not the data intermediary, has the primary responsibility of putting in place adequate security policies and processes. In this case, the Commission found several key issues in the system's policies and processes.

25. First, Cellar Door had not carried out and had no plan on carrying out (prior to the data breach that has happened) penetration testing on the IT system, which

meant that there was no systematic way of identifying vulnerabilities. Further to what was mentioned above at paragraph 22, this posed a limitation to Cellar Door's ability to determine the technical measures that are required to ensure that the personal data held by GIW is adequately protected.

26. Second, Cellar Door did not have an ongoing maintenance process to maintain the website and to regularly update or patch it against the latest risks and vulnerabilities. GIW had informed the Commission that Cellar Door did not sign a maintenance contract with GIW for the maintenance and "upkeeping (sic) of the website and scripts". This was unacceptable as it left the system exposed to new vulnerabilities that regular security patching could have addressed.

27. Third, there was no incident-management policy or process that tracked identification of the technical issues through to their resolution. GIW had essentially left it to its "offshore programmers" to assess how the breach has happened, which came back inconclusive.

28. In the Commission's assessment, given these shortcomings in the policies and processes above, the Respondents, in particular, Cellar Door, did not provide the necessary oversight, accountability, control for the proper protection of the personal data of Cellar Door's customers.

(2) Failure to protect the system against intrusions or attacks

29. Another important aspect of a "reasonable security arrangement" for IT systems is that it must be sufficiently robust and comprehensive to guard against a possible intrusion or attack. For example, it is not enough for an IT system to have strong firewalls if there is a weak administrative password which an intruder can "guess" to enter the system. The nature of such systems require there to be sufficient coverage and an adequate level of protection of the security measures that are put in place, since a single point of entry is all an intruder needs to gain access to the personal data held on a system. In other words, an organisation needs to have an "all-round" security of its system. This is not to say that the security measures or the coverage need to be "perfect", but only requires that such arrangements be "reasonable" in the circumstances.

30. In this case, the Respondents have failed to put such an all-round security in place. The Commission has found several significant gaps in the security measures implemented as follow:

(a) No server firewall installed. While there was an alleged "software firewall configuration", there was no firewall installed to protect GIW's server itself at the material time. A firewall is fundamental to the security of the server to protect against an array of external cyber threats, and GIW has the responsibility of ensuring that such a fundamental measure is in place for its server. In this case, a dedicated firewall (beyond the alleged software firewall configuration) protecting the server itself was only installed after the data breach incident had taken place.

(b) Unused ports were not closed. The unused ports on the server were not closed at the time of the data breach. Leaving unused ports on a server open increases the risk of an external hacker exploiting the services running on these ports. According to Cellar Door, GIW has since then blocked all unnecessary ports on the server.

(c) Login credentials were transferred in clear and unencrypted text. With regard to the Site's functionality, the Commission found that login credentials (ie user logins and passwords) were being transferred in clear and unencrypted text, indicative of a poor level of security in the system design and implementation. This security vulnerability exposed the hosting environment to potential compromise should the credentials be intercepted. Cellar Door, as the organisation having the overall responsibility and control over the design and functionalities of the Site, has the obligation to ensure that, as part of the design and functionalities of the Site, provisions were made for the security of the transmission of the login credentials. In its original design, the Site did not have such a security feature to protect the transmission of the login credentials – but this was prior to Section 24 of the PDPA coming into force on 2 July 2014. However, subsequently when the PDPA came into full effect on 2 July 2014, Cellar Door had the obligation to review the design and functionalities of the Site, and put in place the necessary security arrangements to comply with Section 24 of the PDPA. Yet, Cellar Door had failed to do so, and the Site still lacked in the necessary measures to secure the transmission of the login credentials.

(d) Weak administration password. Another of the corrective actions that the Respondents undertook was to increase the "DB Admin Password", which was only six-characters at the material time. In general, a six-character password is not a strong password. Given that the password was for the admininistration account of a database with remote access capability, the Respondents' password policy should minimally have required a password with a longer length and a mix of alphanumeric and special characters. The need to have a strong password is fundamental to the security of the database system. Weak passwords increase the chances of an intruder cracking the password and gaining full access to the database system, and, more importantly, the personal data stored therein.

31. The security gaps and issues mentioned above exposed the system to all sorts of risks and attacks, such as penetration attacks, cracking, hijacking, and so on and so forth. Ultimately, an intruder that was able to enter through the gaps in the system and gain access to the system would have gained unauthorised access to the personal data held on that system. In the Commission's assessment, therefore, the lack of an all-round security in this case was a breach of Section 24 of the PDPA.

Whether GIW is in breach of Section 24

32. GIW had the direct responsibility of ensuring the protection of the personal data that were in its possession on its servers pursuant to Section 24 of the PDPA. Yet, as set out in paragraphs 29 and 30 above, there were a number of issues pointing towards the lack of protection of the personal data on GIW's servers. In particular, GIW did not put in place adequate security measures when it failed to install a server-side firewall, close unused ports, and implement stronger administration passwords. Accordingly, GIW is in breach of its obligation under Section 24 of the PDPA.

Whether Cellar Door is in breach of Section 24

33. Given that GIW is a data intermediary of Cellar Door, it follows from Section 4(3) of the PDPA, as mentioned above, that Cellar Door is obliged to protect the personal data processed by GIW as if Cellar Door had processed the personal data itself. As such, the Commission's findings regarding the failure by GIW to fulfil its responsibilities and obligations under the PDPA are equally relevant in determining whether there was a breach of the Protection Obligation by Cellar Door. In particular, as mentioned above at paragraph 30(c), it was Cellar Door that had the overall responsibility and control over the requirement of the Site, and it needed to ensure that necessary security measures were in-built in the requirement of the Site, at least since the PDPA came into force.

34. Additionally, Cellar Door had the primary responsibility of ensuring the overall protection of the data under Section 24 of the PDPA, and to implement the overall measures to protect the data. However, as examined at paragraphs 22 to 28 above, Cellar Door failed to implement adequate policies or processes to protect the personal data under its control. Instead, based on the evidence produced in the matter, it was apparent to the Commission that Cellar Door had mainly relied on its data intermediary, GIW, to run its IT and data management system.

35. Accordingly, the Commission finds that Cellar Door had similarly breached its obligations under Section 24 of the PDPA.

D. THE COMMISSION'S DIRECTIONS

36. In assessing the breach and the remedial directions to be imposed, the Commission took into consideration various factors relating to the case, including the mitigating and aggravating factors set out below.

(a) the security measures on the Site to protect the personal data fell below the standard reasonably expected, as highlighted at paragraphs 22 to 31 above, Cellar Door and GIW had inadequate security policies and processes; they failed to protect the system against penetration attacks; and they had a poor admin password policy;

(b) Cellar Door and GIW had shown a lack of awareness or knowledge of required security measures expected over the personal data in the

Site/their hosting environment. As highlighted at paragraphs 6, 24, 31 to 34 above, Cellar Door and GIW were unable to show how the personal data had been taken from the Site or hosting environment, and had not shown to the satisfaction of the Commission that there were sufficient safeguards to prevent this from happening;

(c) Cellar Door and GIW had been neither cooperative nor forthcoming in its responses to the NTPs issued by the Commission as part of its investigation. In this regard, the Commission notes that Cellar Door and GIW displayed a cavalier attitude by providing incomplete responses to the NTPs issued by the Commission; and

(d) although not all the personal data of the customers of Cellar Door had been disclosed on the Pastebin website, given the inadequacies of the Respondents' security measures, the entire customer database was put at risk.

37. Pursuant to section 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that Cellar Door has breached the Protection Obligation under section 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs Cellar Door to do the following:

a. Cellar Door shall within 60 days from the date of the Commission's direction:

i. conduct a vulnerability scan of the Site;

ii. patch all vulnerabilities identified by such scan;

b. Cellar Door shall, in addition, submit to the Commission by no later than 14 days after the conduct of the abovementioned vulnerability scan, a written update providing details on:

i. the results of the vulnerability scan;

ii. the measures that were taken by Cellar Door to patch all vulnerabilities identified by the vulnerability scan; and

c. Cellar Door shall pay a financial penalty of S$5,000.00 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

38. Pursuant to section 29(2) of the PDPA, and having completed its investigations and assessment of this matter, the Commission is satisfied that GIW has breached the Protection Obligation under section 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs GIW to:

a. Pay a financial penalty of S$3,000.00 within 30 days from the date of the Commission's direction, failing which interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

39. In this case, the Commission has awarded a higher penalty amount against Cellar Door as, in the Commission's view, Cellar Door retained the primary responsibility and obligation to protect the personal data of its customers as the data controller, as elaborated at paragraph 15 above.

40. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA, and it urges parties to take the necessary action to ensure that they comply with their obligations under the PDPA.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION