DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1411-A250

[Redacted] (Replaced with Mr X)

… Complainant

AND

(1) Smiling Orchid (S) Pte Ltd (UEN No. 199100754R)

(2) T2 Web Pte Ltd (UEN No. 200510133Z)

(3) Cybersite Services Pte Ltd (UEN No. 201212065M)

(4) East Wind Solutions Pte Ltd (UEN No. 201135906Z)

… Respondents

Decision Citation: [2016] SGPDPC 19

GROUNDS OF DECISION

4 November 2016

A. BACKGROUND

1. On 24 November 2014, the Personal Data Protection Commission (the "**Commission**") received a complaint from the Complainant, Mr X, in relation to the failure of the 1st Respondent, Smiling Orchid (S) Pte Ltd ("**Smiling Orchid**"), a food caterer, to put in reasonable security measures on its website to prevent disclosure of their customers' personal data.

2. Following the Complainant's complaint, the Commission undertook an investigation into the matter. The Commission has determined that there are four respondents in this matter, namely:

   (a) Smiling Orchid;

   (b) T2 Web Pte Ltd ("**T2**");

   (c) Cybersite Services Pte Ltd ("**Cybersite**"); and

   (d) East Wind Solutions Pte Ltd ("**East Wind**").

3. The Commission's decision on the matter and grounds of decision are set out below.

B. MATERIAL FACTS AND DOCUMENTS

4. Smiling Orchid is a food catering company.

5. Smiling Orchid owns the rights to two different domains, namely, smilingorchid.com and smilingorchid.com.sg. Customers can place orders for Smiling Orchid's bakery and catering services through its website.

6. T2 is a web design and development company. By way of a Project Agreement between T2 and Smiling Orchid dated 29 July 2008 ("**Project Agreement**"), T2 was engaged by Smiling Orchid to design the Smiling Orchid webpage and build a Content Management System ("**CMS**") to manage Smiling Orchid's bakery and catering content on its website.

7. T2 created the design and HTML code but outsourced the development of the entire CMS to a freelancer, who in turn subcontracted the actual development of the CMS to another entity that T2 has only identified as "developers based in China". T2 represented that there are no records available about (i) how the CMS was tested by the developer; or (ii) systematic acceptance tests done by the respective contractor.

8. Cybersite was the domain and website hosting provider for Smiling Orchid from 3 April 2014 to 3 April 2016 and had, in its possession, the personal data of Smiling Orchid's customers stored in its servers in Singapore. Since 24 April 2015, Smiling Orchid has changed its hosting providers and T2 has been hosting Smiling Orchid's website via Pozhub Solutions Pte Ltd ("**Pozhub Solutions**"), but Cybersite continued to host the domain name.

9. East Wind is the new IT service provider to Smiling Orchid that was engaged after the occurrence of the data breach complained of by the Complainant to help Smiling Orchid with ensuring basic security and prevention of its portal and infrastructure.

10. On 1 August 2014, the Complainant placed an order on Smiling Orchid's website for a workplace event on 28 August 2014 ("**Order**").

11. On or around 10 November 2014, the Complainant did a random search of his full name on www.yahoo.com.sg. Among the search results was a URL link to a website containing details of the Complainant's Order, including his full name, residential address, mobile number, workplace address and workplace email address (the "**Data Breach Incident**").

12. On 11 and 18 November 2014, the Complainant reported the Data Breach Incident to Smiling Orchid but did not receive any response. Thereafter, the Complainant lodged a complaint with the Commission.

13. Based on the Commission's investigation into the matter, the Commission also found that as at 18 February 2015, the preview order function at the URL http://www.smilingorchid.com/admin/orde/catering/cateringOrderDetail.php?pkid=5893 displayed the order details of other Smiling Orchid customers and that by changing the numerals at the end of the URL, the order details of other customers could be accessed.

14. In November 2015, the Commission noted that the order information was again accessible on Smiling Orchid's website without authentication. In fact, not only could the direct link be used as before, the following alternative link yielded a whole list of orders, which could be accessed from the hyperlinks within that list: http://www.smilingorchid.com/admin/order/catering/cateringOrderList.php.

15. It is not disputed that the details of the customers' orders contained personal data under the control of Smiling Orchid at the material time.

How the Data Breach Incident occurred

16. In its responses to the Commission during the investigation, Smiling Orchid represented that it was only made aware of the Data Breach Incident and the security vulnerability when the Commission informed it of the investigation arising from the Complainant's complaint.

17. Smiling Orchid represented that it had depended on T2 to be "*in charge of the site*" and had expected that T2 would highlight any security issues that Smiling Orchid should have paid attention to. This was despite the fact that (i) the security of the site or the CMS system was not included under T2's scope of work under the Project Agreement; (ii) Smiling Orchid conceded that issues of security did not cross their mind and T2 was engaged mainly to enhance the design of their website; and (iii) Smiling Orchid did not recall discussing any aspects of website security with T2.

18. In turn, T2 denied that it was responsible for Smiling Orchid's website security at the time of the Data Breach Incident and alleged that Cybersite was the party in charge of Smiling Orchid's website security.

19. Cybersite admitted that it was responsible for the security of the hosting system. Cybersite represented that it had employed a basic hosting model using shared services, provided regular security updates of basic hosting provisions such as firewall, anti-virus and anti-spam software and regularly changed the system password as part of its security process. However, Cybersite conceded that it did not conduct regular security testing such as an intrusion test as part of its processes.

20. T2 represented that upon being informed by Smiling Orchid in February 2015 of the Data Breach Incident, T2 conducted investigations and

discovered that the code protecting the site content had been removed. As a result, data which was supposed to be protected and accessible only by users with administrator rights could be accessed by users without such administrator rights. In response, T2 changed the administrator and server passwords and added back the lines of code protecting the site content.

21. T2 also represented that there may have been similar instances where the administrator rights were removed but T2 was not able to provide details of when such incidents occurred. Whenever such an incident occurred, T2 would change the administrator and server passwords, and check and reinstate the codes to secure the website.

22. T2 hypothesised that the Data Breach Incident may have been caused by the following: (i) that hackers compromised the security of the administrator module notwithstanding the existence of the password protection; or (ii) that Smiling Orchid's employees had shared their passwords to the website.

23. With regard to T2's first hypothesis, T2 represented that the CMS was assumed to be designed in such a way that normal usage of the CMS system by staff would not result in changes to the code. The code was intended to be static to such users. However, T2 conceded that as the development of the CMS was outsourced, no test records were available and it did not know how extensively this function had been tested by the developers or contractors.

24. Investigations carried out by Cybersite and the new hosting provider, Pozhub Solutions, disclosed no record of any cyber-attacks to its hosting system for Smiling Orchid between June 2014 and November 2014 when the Data Breach Incident had occurred.

25. In relation to T2's second hypothesis, T2 represented that the administrator password was known to T2, one of the freelancers and to a few people within Smiling Orchid, one of whom has since left Smiling Orchid. Any one of these persons could have created new administrator accounts and passwords. There were no logs that can conclusively rule out this possibility.

26. T2 conceded that there was no known enforcement of password strength or password length within the system. In fact, T2 represented that the password was "likely" part of the PHP framework configuration file and was likely stored in clear text. If not, it would be part of the MySQL database. T2 admitted that it had seen and removed some passwords within the MySQL database.

27. To date, the root cause of the recurring removal of the code which allowed access to the personal data on the database without the administrator password has not been ascertained.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

28. The issues to be determined by the Commission are as follows:

    (a) what obligations did each of the Respondents owe under the Personal Data Protection Act 2012 ("**PDPA**") in respect of the Complainant's personal data; and

    (b) did each of the Respondents comply with its obligation under Section 24 of the PDPA in respect of the Data Breach Incident.

29. Section 24 of the PDPA provides that an organisation shall 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 ("**Protection Obligation**").

30. Section 2(1) of the PDPA defines a "data intermediary" as an organisation which processes personal data on behalf of another organisation but does not include an employee of that organisation. Processing personal data on behalf of another organisation refers to the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, the organisation, adaptation or alternation; retrieval; and transmission of the said personal data.

31. 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.

32. In addition, 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.

<u>Issue (a): what obligations did each of the Respondents owe under the PDPA in respect of the Complainant's personal data?</u>

Smiling Orchid

33. It is not disputed that Smiling Orchid, being an organisation which has its customers' personal data in its possession and/or under its control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, pursuant to section 24 of the PDPA.

34. This is so regardless of whether Smiling Orchid had appointed a data intermediary or data intermediaries to process customer personal data

on its behalf. As such, Smiling Orchid is required to comply with section 24 of the PDPA and adopt or ensure the adoption of security arrangements that are reasonable and appropriate in the circumstances.

T2

35. In light of the facts and representations made by Smiling Orchid and T2, the Commission understands that T2 had not been engaged by Smiling Orchid to carry out any processing activities with regard to personal data on its behalf. Therefore, it cannot be said that T2 is a data intermediary processing personal data on behalf of Smiling Orchid.

36. First, as noted at paragraph 17 above, the security of the site or the CMS system was not part of T2's scope of work under the Project Agreement and Smiling Orchid conceded that T2 was engaged mainly to enhance the design of its website.

37. Second, the Commission notes that T2 did not deal with any personal data of Smiling Orchid's customers. Accordingly, none of the Complainant's personal data can be said to have been in T2's possession or under T2's control at the material time.

38. Hence, even though Smiling Orchid represented that it had depended on T2 to be "*in charge of the site*" and T2 itself represented that it had investigated the cause of the Data Breach Incident and carried out corrective measures upon being informed of the Data Breach Incident in February 2015 and on other occasions, the Commission is satisfied that there was no evidence that T2 was charged with the responsibility to secure the personal data as a data intermediary.

39. Accordingly, T2 did not have an obligation under Section 24 of the PDPA to protect the personal data on Smiling Orchid's website.

Cybersite

40. The Commission considers that Cybersite was a data intermediary of Smiling Orchid for the purposes of the PDPA. Cybersite was the hosting service provider for Smiling Orchid's website at the material time and, as noted at paragraph 8 above, it had in its possession the personal data of Smiling Orchid's customers stored in its servers in Singapore.

41. Pursuant to Sections 4(2) and 4(3) of the PDPA, Cybersite had an obligation to make reasonable security arrangements to protect the personal data of Smiling Orchid's customers.

East Wind

42. East Wind is a data intermediary of Smiling Orchid for the purposes of the PDPA as it is an IT service provider and processed personal data on behalf of Smiling Orchid.

43. Since East Wind was only appointed by Smiling Orchid after the Data Breach Incident and was not involved in any part of the site during the material time, the Commission is of the view that East Wind's role does not factor into its considerations pertaining to the Data Breach Incident.

Issue (b): did each of the Respondents comply with their obligation under Section 24 of the PDPA in respect of the Data Breach Incident?

Smiling Orchid

44. After carefully considering all the relevant facts and representations made by the Respondents, the Commission is of the view that Smiling Orchid failed to take reasonable security measures to protect the customers' personal data in its possession and/or under its control.

45. First, the Commission found that there was no clear designation of security responsibilities by Smiling Orchid. As noted at paragraphs 17 and 18 above, Smiling Orchid represented that it had depended on T2 to be "*in charge of the site*" but T2 denied that it was responsible for Smiling Orchid's website security at the time of the Data Breach Incident.

46. As an organisation subject to the data protection provisions of the PDPA, Smiling Orchid is ultimately responsible for ensuring that there are reasonable security arrangements in place to protect the personal data in its possession and/or under its control; further, that any data intermediary that processes personal data on its behalf complies with the PDPA. In this case, it would appear that prior to the Commission's investigation, Smiling Orchid had not even considered that it was required to implement reasonable security measures to ensure that the personal data in its possession and/or under its control was adequately protected in accordance with Section 24 of the PDPA. Smiling Orchid had merely relied on T2 to be "*in charge of the site*" without properly engaging T2 to provide security oversight for the site. The omission to do so discloses the lack of implementing security arrangements for the site.

47. Second, the investigations undertaken by T2 were poorly conducted and the corrective actions it performed by reinserting the line of code and changing the administrator and server passwords were superficial and did not address the root cause of the incident. Consequently, a breach caused by the same the line of code being removed had occurred again in November 2015 and T2 had again performed the same ineffective corrective actions. That the line of code had been removed on more than one occasion showed that Smiling Orchid had failed to ensure that adequate corrective actions were performed to resolve the root cause of any unauthorised access and/or disclosure. It also demonstrated an inadequate understanding of IT security that fell below reasonably expected standards.

48. Third, even though the issue was made known to Smiling Orchid in November 2014, even as late as October 2015, Smiling Orchid had only undertaken corrective actions in one domain even though there were two domains involved. The same security issue had also arisen again in November 2015 even after the whole system was ported to a new hosting environment. Furthermore, since T2 has yet to identify the actual cause of the code removal, Smiling Orchid is unable to say that the corrective actions that T2 had undertaken would be enough to address this problem.

49. In addition, as noted at paragraph 26 above, T2 admitted that the protection of accounts and passwords were weak: i.e. CMS passwords, including the administrator user passwords were stored in plain text and were unprotected, and there was a lack of a policy relating to password length nor strength.

50. New administrator accounts and passwords in relation to the CMS could be created by any existing administrator account holder and there was no indication of any policy or logs as to who maintains these accounts and removes unused accounts. While the absence of a policy for the protection and accountability of the administrator user accounts is not directly related to the cause of the Data Breach Incident, the Commission is of the view that this demonstrates an overall lack of security awareness on the part of Smiling Orchid and a failure to make reasonable security arrangements.

51. It is unclear whether T2's actions would have been different had it been engaged to do more than enhancing the design of the site. Data controllers that engaged outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services. In the absence of such clarity of intent and procedures, it is risky to hold that the outsourced service provider is a data intermediary. In any case, the Commission has found that T2 is not a data intermediary for the reasons set out at paragraphs 35 to 38 above.

52. Consequently, in view of all the relevant facts and circumstances, the Commission is not satisfied that Smiling Orchid has made reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks in compliance with the Protection Obligation under Section 24 of the PDPA.

Cybersite

53. As a data intermediary of Smiling Orchid, Cybersite has an obligation to comply with the Protection Obligation under Section 24 of the PDPA.

54. In this case, there was no evidence of Cybersite being in breach of its Protection Obligation under Section 24 of the PDPA.

55. For the general security of its servers, Cybersite had put in place security arrangements including regular changing of system passwords, and regular updates of its firewall(s), anti-virus software, anti-spam software. There was no evidence that these security measures had been compromised or of Cybersite's servers being hacked at the material time.

56. Relating to the data breach that had occurred in this case, the security issues that were identified were at the application-level (i.e. the CMS system). It was found that these issues did not pertain to the contracted responsibilities of Cybersite, who was only hosting the site. Although T2 had hypothesised that the code was removed because someone had hacked into the system by gaining access to Cybersite's servers where the code is stored to remove the code, as mentioned above, there was no evidence of cyber-hacking into Cybersite's servers at the material time. In any event, the same issue occurred even after Smiling Orchid had switched hosting service providers.

57. Accordingly, the Commission does not find Cybersite to be in breach of Section 24 of the PDPA.

D. ENFORCEMENT ACTION TAKEN AGAINST SMILING ORCHID

58. Having completed its investigation and assessment of this matter, the Commission finds that Smiling Orchid is in breach of Section 24 of the PDPA.

59. In exercise of the power conferred upon the Commission pursuant to Section 29 of the PDPA, the Commission directs that a financial penalty of S$3,000 be imposed on Smiling Orchid.

60. The Commission also directs that:

(a) Smiling Orchid shall, within 120 days from the date of the Commission's direction:

(i) put in place the security arrangements for the new website to protect the personal data that was collected, or may be collected, by Smiling Orchid;

(ii) conduct a web application vulnerability scan of the new website;

(iii) patch all vulnerabilities identified by such vulnerability scan; and

(b) by no later than 14 days after the above action has been carried out, Smiling Orchid shall, in addition, submit to the Commission a

written update providing details on (i) the results of the vulnerability scan; and (ii) the measures that were taken by Smiling Orchid to patch all vulnerabilities identified by the vulnerability scan.

61. The Commission took into account the following factors in assessing the breach and the directions to be imposed:

Smiling Orchid

(a) Smiling Orchid was not forthcoming nor cooperative in providing the full details of what transpired and its IT outsourcing agreements during the Commission's investigation. In fact, despite the issuance of one Notice to Require Production of Documents and Information to Smiling Orchid and several verbal clarifications over the phone, the Commission was still unable to establish the pertinent facts on what caused the discourse and the specific roles of the parties involved at the material time. As a result, the Commission had to take statements from the relevant parties in order to gather and distil facts;

(b) there was a recurring breach of the exact same nature in November 2015, even after Smiling Orchid had been informed of the Data Breach Incident by the Commission in February 2015. Every time a data breach occurred, the same ineffective corrective action would be taken by putting back the lines of codes protecting the site content by the administrator password without ascertaining the root cause of the repeated breaches;

(c) Smiling Orchid's entire database was potentially at risk of being disclosed if someone possessed the know-how to change the digits in the URL link;

(d) even though Smiling Orchid is a small-medium enterprise without internal IT knowledge and expertise, as an organisation under the PDPA, it is ultimately responsible for protecting the personal data in its possession and/or under its control pursuant to Section 24 of the PDPA;

(e) the impact of the data breach appears to have been limited; and

(f) Smiling Orchid has taken some steps to remedy the breach, including engaging a new IT vendor, East Wind, to revamp Smiling Orchid's website.

T2 and Cybersite

62. The Commission finds that T2 and Cybersite appeared to play a significant role in this matter. T2 was essentially Smiling Orchid's main IT vendor and Smiling Orchid was heavily dependent on T2 in respect of

its entire IT system. However, T2 had a superficial understanding of the IT system. Its repeated outsourcing of different tasks to different parties, who in turn re-outsourced the tasks, also resulted in confusion as to which party was responsible for the defective line of code that eventually led to the Data Breach Incident. Notwithstanding, as T2 was only engaged to provide web designing services and not website security and it did not handle or process personal data at the material time of the Data Breach Incident, the Commission finds that T2 was not a data intermediary of Smiling Orchid and was not in breach of the Protection Obligation under the PDPA.

63. Cybersite, which was the domain and hosting provider for Smiling Orchid, also has an important role to protect the personal data of Cybersite's customers that were held on its servers. Although the Commission has not found Cybersite to be in breach of the Protection Obligation under Section 24 of the PDPA, the Commission is of the view that a timely reminder should be issued to the organisation on its obligation as a domain and hosting provider in view of the data breach that had taken place.

64. The Commission will be issuing advisory notices to T2 and Cybersite on their roles and obligations mentioned above.

East Wind

65. The Commission notes that East Wind was Smiling Orchid's newly-appointed IT vendor that provided assistance and support in terms of security know-how during the investigation and was not involved in any way at the material time.

66. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION