DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1410-A163

(1) FU KWEE KITCHEN CATERING SERVICES (UEN No. 52824092K)

(2) PIXART PTE. LTD. (UEN No. 201011239D)

…Respondents

Decision Citation: [2016] SGPDPC 14

GROUNDS OF DECISION

21 September 2016

Background

1. On 30 September 2014, the Personal Data Protection Commission ("**Commission**") received a complaint against Fu Kwee Kitchen Catering Services ("**Fu Kwee**") regarding an alleged data breach by Fu Kwee involving unauthorised access of Fu Kwee's customers' personal data.

2. The Commission commenced an investigation under section 50 of the Personal Data Protection Act 2012 ("**PDPA**") to ascertain whether there had been a breach by Fu Kwee and/or Pixart Pte. Ltd. ("**Pixart**") (the Respondents in this investigation) of their respective obligations under the PDPA.

Material Facts and Documents

Fu Kwee's relationship with Pixart

3. Fu Kwee provides food and beverage catering services in Singapore. It owned and managed the following website at the material time of the complaint: http://www.fukweecatering.sg, where different customer orders could be viewed through at the following URLs http://www.fukweecatering.sg/fixmenu1preview.aspx?pid=[number].

4. Pixart is an IT vendor engaged by Fu Kwee in 2010 to (a) develop an online ordering system for Fu Kwee and Fu Kwee's corporate website, and (b) host, support and maintain the website. The PDPA came fully

into force on 2 July 2014, and as the contract between Fu Kwee and Pixart was only terminated sometime around April or May 2015, Pixart remained responsible for hosting, supporting and maintaining the website at the time of the alleged data breach incident in September 2014.

Data breach incident

5. The Complainant stated that she was a customer of Fu Kwee, and alleged that she could retrieve another customer's order details and personal data (specifically the customer's name, postal address and personal contact number) by changing the numerals at the end of the URL of Fu Kwee's order preview webpage at http://www.fukweecatering.sg/fixmenu1preview.aspx?pid=102 from "102" to "97"[1] (i.e. http://www.fukweecatering.sa/fixmenu1preview.aspx?pid=97).

6. At the material time, on 17 September 2014, while Fu Kwee had a default anti-virus programme for its server, it did not implement any measures to protect its customers' personal data from unauthorised access through the type of vulnerability discovered by the Complainant (ie that the personal data of other customers could be viewed by altering the numerals at the end of the URL for Fu Kwee's order preview webpage).

7. Fu Kwee appeared to be unaware of this vulnerability until the Commission issued its first Notice to Require Production of Documents and Information on 12 December 2014 ("**First NTP**"). Fu Kwee then instructed Pixart to address the vulnerability on 30 December 2014. No notifications were sent by either Fu Kwee or Pixart to the customers affected by the data breach.

8. Pixart confirmed, from its checks on the system, that the URL of each order preview webpage that was generated after a customer's order did not expire. Pixart also confirmed that the URL of the order preview webpage would include the customer's order ID number, which was as short as three digits and generated sequentially via Fu Kwee's website. This enabled anyone who had a pre-existing URL to access other customers' orders and their personal data simply by altering the numerals at the end of the URL of Fu Kwee's order preview webpage.

9. Pixart implemented a "one-time URL" solution on 30 December 2014. This technical solution incorporates a 20-minutes exposure security feature that permits a customer to view his or her own order only once before the URL automatically expires after 20 minutes. The URL would

also similarly expire if the webpage was closed or refreshed by the customer.

10. Investigations revealed that the scope of the contract between Fu Kwee and Pixart did not include the implementation of security measures on Fu Kwee's website to protect customers' personal data. Pixart had also not conducted any penetration tests on Fu Kwee's website. Such penetration tests could have enabled Fu Kwee to discover the design flaw of its order preview webpages.

11. Additionally, in the course of the investigations, Fu Kwee was found not to have implemented any password policy to restrict or control staff access to its database of customers' personal data. Fu Kwee also neither implemented personal data protection policies for the collection, use or disclosure of personal data nor appointed a data protection officer to safeguard its customers' personal data ("**DPO**").

12. Having carefully considered the relevant facts and circumstances, including the statements and representations made by Fu Kwee and Pixart, the Commission sets out its findings and assessment herein.

THE COMMISSION'S FINDINGS AND ASSESSMENT

Issues for determination

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

    (a) Whether Fu Kwee had breached the obligation under section 24 of the PDPA (the "**Protection Obligation**");

    (b) Whether Fu Kwee had breached the obligation under sections 11 and 12 of the PDPA (the "**Openness Obligation**"), specifically, sections 11(3) and 12(a), for failure to appoint a DPO and put in place privacy policies and practices, in contravention of those sections of the PDPA;

    (c) Whether Pixart is a data intermediary of Fu Kwee; and

    (d) Whether Pixart had breached the Protection Obligation.

Issue A: Whether Fu Kwee had breached the Protection Obligation

14. Section 24 of the PDPA states:

> "***Protection of Personal Data***
> *24. 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."*

15. Pursuant to section 24 of the PDPA, Fu Kwee, being an organisation which had its customers' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Protection Obligation applies equally to all personal data in the possession or under the control of the organisation, including personal data that the organisation may have collected before 2 July 2014, when the data protection provisions under Parts III to VI of the PDPA came into effect.

16. Following a careful assessment of the relevant facts and circumstances, the Commission is of the view that Fu Kwee had not reasonably discharged its obligation under section 24 of the PDPA until the fixes introduced on 30 December 2014. In particular, the Commission has identified the following vulnerabilities in Fu Kwee's security arrangements, which illustrate how Fu Kwee failed to make reasonable security arrangements to protect customers' personal data:

    (a) Fu Kwee's website did not require password access, which could have reasonably restricted unauthorised access to customers' personal data using the website.

    (b) The order preview URLs that were generated by Fu Kwee's website whenever a customer placed an order not only did not expire, but were also predictable. This enabled any customer to simply alter the last few digits of an order preview URL in order to access the order details and personal data of other customers.

    (c) Fu Kwee acknowledged that it had not instructed Pixart to put in place security measures to protect its customers' personal data even after 2 July 2014, when the data protection obligations in the PDPA came into force.

(d) The investigations also found that there were no access controls to Fu Kwee's database of customers' personal data. Accordingly, though Fu Kwee had sought to protect its server containing the database using a default Windows firewall, the database remained vulnerable to unauthorised access.

17. The vulnerabilities set out above demonstrate that Fu Kwee could have done more to protect its customers' personal data that was in its possession or under its control. When viewed in totality, the Commission is of the view that Fu Kwee had failed to make reasonable security arrangements to protect its customers' personal data because these vulnerabilities were preventable.

18. Although Fu Kwee had outsourced the hosting, support and maintenance of its online ordering system and corporate website to Pixart (which the Commission has determined to be a data intermediary of Fu Kwee for the reasons set out below), Fu Kwee was ultimately responsible for the security of the website and customers' personal data as if the personal data was processed by Fu Kwee itself (per section 4(3) of the PDPA).

19. In light of the foregoing, the Commission finds that Fu Kwee had breached the Protection Obligation at the material time.

Issue B: Whether Fu Kwee had breached the Openness Obligation

20. Sections 11 and 12 of the PDPA together constitute the Openness Obligation under the PDPA, which provides that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA, and shall make information about its policies and procedures publicly available. In particular, section 11(3) of the PDPA provides that an organisation shall designate one or more individuals as a DPO to be responsible for ensuring that the organisation complies with the PDPA. In the same vein, section 12(a) of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisations under the PDPA.

21. Fu Kwee confirmed that between 2 July 2014 and 12 December 2014, Fu Kwee neither implemented any personal data protection policies for the collection, use or disclosure of personal data, nor appointed a DPO.

22. In light of the foregoing lapses, the Commission finds that Fu Kwee had breached the Openness Obligation.

Issue C: Whether Pixart is a data intermediary of Fu Kwee

23. Under section 2(1) of the PDPA, a "*data intermediary*" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. The term "*processing*" in relation to personal data means the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, any of the following: recording; holding; organisation, adaptation or alteration; retrieval; combination; transmission; erasure or destruction. Section 4(2) of the PDPA imposes on a data intermediary the obligation to protect personal data under section 24 of the PDPA and the obligation to cease to retain personal data under section 25 of the PDPA in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. Save for the aforementioned obligations, Parts III to VI of the PDPA do not impose any other obligations on the data intermediary, in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced and made in writing.

24. Based on the facts and representations by Fu Kwee and Pixart, the Commission notes that Pixart was contractually engaged by Fu Kwee in 2010 to (a) develop an online ordering system for Fu Kwee and Fu Kwee's corporate website, and (b) host, support and maintain Fu Kwee's website. As the contract was only terminated sometime in April/May 2015, Pixart was still responsible for hosting, supporting and maintaining Fu Kwee's corporate website and ordering system at the material time of the data breach incident in September 2014.

25. The Commission is of the view that Pixart had processed personal data of Fu Kwee's customers, pursuant to the contract between Fu Kwee and Pixart in relation to the hosting, support and maintenance of the online ordering system and Fu Kwee's corporate website, and Pixart had done so on behalf of and for the purposes of Fu Kwee.

26. In this regard, the Commission finds that Pixart was acting as a data intermediary of Fu Kwee with respect to the relevant websites at the URLs set out above in connection with the data breach incident, as Pixart essentially processed Fu Kwee's customers' personal data on behalf of

and for the purposes of Fu Kwee in hosting, supporting and maintaining the online ordering system and Fu Kwee's website.

Issue D: Whether Pixart had breached the Protection Obligation

27. Section 24 read with section 4(2) of the PDPA imposes a Protection Obligation on data intermediaries in that a data intermediary is obliged to make "*reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".* In view of the Commission's finding that Pixart was a data intermediary of Fu Kwee at the material time of the data breach incident, Pixart was required to comply with the Protection Obligation under section 24 of the PDPA to protect the personal data it was processing on behalf of and for the purposes of Fu Kwee.

28. In the Commission's view, as a data intermediary, Pixart had an obligation to protect the personal data of Fu Kwee's customers using the ordering system on Fu Kwee's website. Pixart has clearly not discharged the Protection Obligation imposed on it under the PDPA, as it did not have in place reasonable measures to protect the personal data that it was processing for and on behalf of Fu Kwee when it developed, hosted, maintained and provided support in relation to the online ordering system and Fu Kwee's website.

29. In this connection, the Commission notes that if Pixart had advised Fu Kwee on its obligations to protect personal data, but Fu Kwee had rejected Pixart's advice, this could have been taken into account by the Commission as a mitigating factor. However, there is presently no evidence before the Commission suggesting that Pixart had actually advised Fu Kwee on the need to have in place adequate security measures to protect the personal data of Fu Kwee's customers in Fu Kwee's database.

30. In light of the above, the Commission finds that there had been a breach of the Protection Obligation under section 24 of the PDPA by Pixart.

THE COMMISSION'S DIRECTIONS

31. 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.

Fu Kwee's breach of the Protection Obligation and the Openness Obligation

32. In relation to Fu Kwee's breach of the Protection Obligation and Openness Obligation, the Commission took into account the following factors:

(a) Although Fu Kwee had ample opportunity to put in place reasonable security measures from 2 January 2013 to 2 July 2014, or even after 2 July 2014, when the data protection provisions of the PDPA came into force, it did not do so;

(b) Fu Kwee's disregard for its obligations under the PDPA is also apparent as it had failed to appoint a DPO or put in place policies and practices to comply with the PDPA as at June 2015 (when it appointed a new vendor), even after being notified about the data breach incident in December 2014 by the Commission;

(c) Fu Kwee was not forthcoming in providing information during the investigation, and only provided bare facts in its responses during the investigations; and

(d) Notwithstanding that the Commission did not receive any other complaints regarding the relevant websites at the URLs described above, the lapses by Fu Kwee meant that anyone who had the exact URL or who had correctly guessed the parameters could potentially access all the personal data of Fu Kwee's customers who had placed orders online at Fu Kwee's website.

Pixart's breach of the Protection Obligation

33. In relation to Pixart's breach of the Protection Obligation, the following factors were taken into consideration:

(a) Pixart was not forthcoming in providing information during the investigation, and did not respond to the Second Notice to Require Production of Documents and Information dated 10 March 2015, which was addressed to Pixart; and

(b) Pixart took active steps to fix the vulnerability in about two weeks after the Commission informed Fu Kwee about the data breach. Based on the Commission's assessment, the remedial actions taken were acceptable.

34. Having completed its investigation and assessment of this matter, the Commission is satisfied that Fu Kwee had been in breach of the Protection Obligation under Section 24 of the PDPA, and the Openness Obligation under sections 11(3) and 12(a) of the PDPA for the reasons cited above. Pursuant to section 29 of the PDPA, the Commission hereby directs Fu Kwee to do as follows:

(a) Pay a financial penalty of $3,000 within 30 days from the date of the Commission's direction;

(b) For all employees of Fu Kwee handling personal data to attend a training course on the obligations under the PDPA and the organisation's data protection policies and practices within 6 months from the date of the Commission's direction;

(c) Conduct a security audit of the website at http://fukweecatering.com.sg/ to be performed by duly qualified competent contractors or staff. Fu Kwee is to furnish to the Commission, within 30 days from the date the Commission's direction, a schedule stating the scope of the risks to be assessed and the time within which a full report of the audit can be provided to the Commission, and to confirm in the said report that Fu Kwee no longer stores any personal data of its customers on its website; and

(d) To take steps to appoint a DPO and to develop and implement policies and practices that are necessary for Fu Kwee to comply fully with its obligations under the PDPA, and to provide the Commission with a compliance status update within 30 days from the date of the Commission's direction.

35. The Commission is also satisfied that Pixart has not complied with the Protection Obligation under section 24 of the PDPA for the reasons cited above. Pursuant to Section 29(2) of the PDPA, the Commission hereby directs that a financial penalty of S$1,000 be meted out against Pixart.

36. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION

[1] The URL had been taken down shortly after the data breach incident.