DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1409-A103

(1) CHALLENGER TECHNOLOGIES LIMITED (U.E.N. 198400182K)
(2) XIRLYNX INNOVATIONS (U.E.N. 52942580K)

…Respondents

Decision Citation: [2016] SGPDPC 6

GROUNDS OF DECISION

20 April 2016

BACKGROUND

1. The Personal Data Protection Commission (the "**Commission**") received a complaint from a member of the public on 15 September 2014 concerning an alleged data breach by Challenger Technologies Limited ("**Challenger**"). In brief, the complainant alleged that Challenger had sent email communications to members of its ValueClub programme, which contained the personal data of another ValueClub member.

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 Challenger of its obligations under the PDPA.

3. In the course of its investigation, the Commission found that the email communications in question (which were sent to Challenger's ValueClub members) had been sent by Xirlynx Innovations ("**Xirlynx**"), a business engaged by Challenger to handle all its email communications to members of Challenger's ValueClub programme. The Commission's investigation therefore also examined whether there had been a breach by Xirlynx of its obligations under the PDPA.

4. The Commission's findings are set out below.

MATERIAL FACTS AND DOCUMENTS

5. Challenger is a retailer of information technology ("**IT**") and other electronic products with several outlets around Singapore. As part of its customer relations efforts, Challenger established a customer membership programme known as ValueClub, which provides members with membership savings and discounts (amongst other benefits), and enables them to earn and accumulate ValueClub programme points which may be redeemed to offset the cost of purchases made at Challenger outlets.

6. Xirlynx is a third party IT vendor, which is registered and managed by its sole proprietor, [Redacted] (Replaced with Mr T).

7. Some time in or around March 2010, Challenger engaged Xirlynx to manage and execute Challenger's email campaigns under a contract for an "Email Blasting Package". The services provided by Xirlynx to Challenger under the contract included managing Challenger's ValueClub membership database and sending Challenger's weekly advertisements of promotions and monthly ValueClub e-statements to ValueClub members.

8. Challenger thereafter periodically renewed its "Email Blasting Package" contractual engagement with Xirlynx for the latter to send email communications to ValueClub members, including the email communications which are the subject of the Commission's present investigation.

9. In September 2014, Xirlynx sent the monthly ValueClub e-statements for that month to the ValueClub members by email (the "**September Emails**"). However, many of the September Emails contained personal data of another ValueClub member, including their name, expiry date of their ValueClub membership and total number of ValueClub programme points accumulated by the other member.

How the Data Breach Occurred

10. In Challenger's responses to the Commission during the investigation, Challenger indicated that it had, upon being notified of the matter by the Commission, informed [Redacted] (Replaced with Mr T) of Xirlynx about the alleged breach because Xirlynx managed Challenger's ValueClub membership database and was the party responsible for sending out email communications to the ValueClub members. Challenger also conducted an internal investigation to ascertain the cause of the data breach.

11. Following its internal investigation, Challenger represented to the Commission that the root cause of the data breach was a processing error by their vendor, Xirlynx.

12. Challenger also represented to the Commission that it had taken remedial actions to inform the affected ValueClub members regarding the data breach and to rectify the mistakes caused by Xirlynx's error. In addition, Challenger represented that it had taken the extra precautionary step of terminating Xirlynx's services upon discovering the cause of the data breach, and it reviewed its ValueClub communication processes to prevent a reoccurrence of the data breach.

13. Separately, in Xirlynx's responses to the Commission during the investigation, Xirlynx explained that in September 2014, it had been instructed by Challenger to email that month's ValueClub e-statements to ValueClub members. Xirlynx further explained that the following steps comprise its usual workflow for sending the ValueClub e-statements to ValueClub members:

(a) Xirlynx would receive a copy of the contents for the ValueClub e-statements from Challenger one day before the intended email blast.

(b) Xirlynx would adapt the contents received from Challenger into a ValueClub e-statement HTML template. At this point, variables such as members' names, the expiry date of their ValueClub membership and their total number of existing ValueClub programme points, would have not yet been inserted into the HTML template.

(c) Xirlynx would then send the adapted layout to Challenger for its approval. Upon approval, Challenger would send to Xirlynx its updated ValueClub membership database with the latest ValueClub programme points for each members, listed in a text file (.txt) format.

(d) As Challenger's membership database contains duplicate email addresses, Xirlynx would import the database into an Excel worksheet and remove any duplicates using Excel's "Remove Duplicates" function.

(e) The scrubbed database would then be imported into Xirlynx's email blast system, and the ValueClub e-statements sent out to the ValueClub members.

14. For the September 2014 ValueClub e-statements, Xirlynx explained that it had carried out the usual steps listed above. However, while using the "Remove Duplicates" function in Excel to remove the email duplicates from Challenger's membership database, Xirlynx admitted that it had inadvertently also caused an Excel column in the worksheet containing a list of ValueClub members' names, and an Excel column containing a list of the members' email addresses, to be mismatched. This mix up resulted in some ValueClub members' personal data, specifically, their names, ValueClub membership expiry dates and ValueClub programme points being sent to other ValueClub members in the September Emails. In short, Xirlynx's error in the processing of the membership database led to the occurrence of the data breach.

15. Xirlynx informed the Commission that ValueClub e-statements with personal data of another ValueClub member had been sent to 165,306 ValueClub members. Xirlynx further represented that "only 34,230 recipients [of the September Emails] that had opened the e-statements were affected". The Commission understands that Xirlynx derived this smaller number from its data on the number of ValueClub e-statements in the September Emails which were actually accessed by the ValueClub members. The Commission notes that this does not take into account the possibility of additional members accessing the emails in the future. On balance, the Commission is of the view that since the September Emails had been sent to 165,306 ValueClub members and would likely remain in their email account until accessed or deleted by those members, it cannot be said that only 34,320 members were affected. The Commission therefore takes the view that 165,306 members' personal data had been disclosed to other members.

COMMISSION'S FINDINGS AND ASSESSMENT

Issues to be determined

16. The ValueClub e-statements sent in the September Emails each contained a data set that identified another ValueClub member (who was an individual) by his or her full name, and provided the details of the member's accumulated ValueClub programme points and the expiry date of the member's ValueClub membership. The contents of the e-statements therefore come within the definition of "personal data" in section 2(1) of the PDPA.[1]

17. Under section 24 of the PDPA, an organisation is required 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.

18. Accordingly, a key issue in this case is whether Xirlynx had breached its obligations under section 24 of the PDPA.

19. Although Xirlynx had sent the September Emails to ValueClub members, the Commission notes that Xirlynx was processing Challenger's ValueClub members' database and sending the September Emails to the ValueClub members for Challenger pursuant to their contract. Related to this, section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of personal data that is processed on its behalf and for its purposes by a data intermediary as if the personal data was processed by the organisation itself.

20. As such, two additional issues in this case are:

    (a) Whether Xirlynx was a data intermediary of Challenger in respect of the events that caused the data breach; and

    (b) If so, whether Challenger had breached its obligations under section 24 of the PDPA.

The Commission's Decision on the Issues

Whether Xirlynx is a data intermediary of Challenger

21. 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.[2]

22. Section 2(1) also defines the term "*processing*", in relation to personal data, to mean the carrying out of any operation or set of operations in relation to the personal data including, but not limited to, any of the following:

    (a) Recording;
    (b) Holding;

(c) Organisation, adaptation or alteration;
(d) Retrieval;
(e) Combination;
(f) Transmission;
(g) Erasure or destruction.[3]

23. Having reviewed the "invoice no. 2013-01549 from Xirlynx to Challenger dated 31 December 2013", and a "non-disclosure agreement dated 24 April 2014, entered into by [Redacted] (Replaced with Mr H) and [Redacted] (Replaced with Mr T)on behalf of Challenger and Xirlynx respectively" which was provided by Xirlynx to the Commission, and based on the facts set out at paragraph 13, the Commission is of the view that Xirlynx had processed personal data of Challenger's ValueClub members pursuant to the arrangement between Xirlynx and Challenger and they had done so on behalf of Challenger. Further, Challenger had clearly relied on Xirlynx to process its ValueClub members' personal data to send the email communications in question. Xirlynx was therefore a data intermediary of Challenger for the purposes of the PDPA.

24. As Xirlynx was a data intermediary of Challenger, Challenger has the same obligations under the PDPA in respect of Xirlynx's processing of personal data, as if the personal data had been processed by Challenger (per section 4(3) of the PDPA).

25. However, this does not affect Xirlynx's obligations under section 24 of the PDPA as that section applies equally to data intermediaries who process personal data on behalf of and for the purposes of another organisation pursuant to a contract in writing. In this regard, section 4(2) of the PDPA excludes the application of Parts III to VI of the PDPA, except for sections 24 and 25, to such data intermediaries.

Whether Xirlynx had breached section 24 of the PDPA

26. The fact that a data breach had occurred was undisputed by both Xirlynx and Challenger. The Commission therefore considered whether Xirlynx had made reasonable security arrangements to prevent the data breach from taking place.

27. From Xirlynx's representations to the Commission, it was clear that it fell on Xirlynx, as part of its email blasting services, to ensure that the correct individualised ValueClub e-statement was sent to the correct intended recipient. Xirlynx's use of the Excel duplicate removal function while processing Challenger's ValueClub members database was part of this service.

28. It was therefore Xirlynx's responsibility to ensure that processing of Challenger's ValueClub members database was done in the correct manner so as to ensure that the correct set of personal data was sent by Xirlynx to each ValueClub member. The occurrence of the data breach is a *prima facie*

indication that Xirlynx had not fulfilled its responsibilities in respect of processing and sending personal data.

29. The Commission further notes that Xirlynx's error could have been caught if it had proof read random samples of the ValueClub e-statements before the e-statements were sent out to verify that the names of the individuals in the e-statements matched the email addresses to which the e-statement was sent.

30. Sample proof-reading was a reasonable security arrangement that could have been conducted by Xirlynx given the nature of the services it provided, and which would likely have either averted the data leak or greatly reduced the number of individuals affected. The sample size should be appropriate relative to the total number of recipients.

31. Accordingly, the Commission takes the view that by failing to ensure that the correct personal data was sent to ValueClub members via the September Emails, Xirlynx had breached its obligations under section 24 of the PDPA.

Whether Challenger had breached its obligation under section 24 of the PDPA

32. In light of the Commission's above finding that Xirlynx is a data intermediary of Challenger, it follows from section 4(3) of the PDPA that Challenger is obliged to protect the personal data administered by Xirlynx as if Challenger had processed the personal data itself. Section 4(3) of the PDPA states:

"An organisation shall have the same obligation under this Act in respect of 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**." (Emphasis added.)

33. The Commission's findings regarding the failure by Xirlynx to fulfil its responsibilities and obligations under the PDPA are therefore equally relevant in determining whether there was a breach of section 24 of the PDPA by Challenger.

34. In addition, the Commission notes that Challenger had heretofore neglected to exercise control over Xirlynx's workflow in the processing of Challenger's ValueClub membership database and the sending of email communications to ValueClub members. Challenger had left it to Xirlynx to implement measures required to protect the personal data Xirlynx processed and, until the data breach occurred, had not considered what requirements it would want to implement to ensure that the personal data was appropriately protected, in accordance with section 24 of the PDPA.

35. Accordingly, the Commission is of the view that Challenger had similarly breached its obligation under section 24 of the PDPA.

ENFORCEMENT ACTION BY THE COMMISSION

36. Given the Commission's findings that both Challenger and Xirlynx were in breach of their respective obligations under section 24 of the PDPA, the Commission is empowered under section 29 of the PDPA to issue such directions as it deems fit to ensure compliance with the PDPA. This may include directing either or both parties to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

37. In considering whether to give such a direction in this case, the Commission notes the following:

    (a) The personal data leaked was limited (comprising only ValueClub members' names, their membership expiry dates, and accumulated ValueClub programme points) and not of a sensitive nature;

    (b) The personal data leaked could not be used by the individuals who had received them to profiteer or benefit from them, and was unlikely to lead to any harm or loss to the individuals concerned; and

    (c) Both Xirlynx and Challenger had been cooperative with the Commission and forthcoming in their responses to the Commission during the Commission's investigation.

38. The Commission also notes that Challenger had taken several proactive steps to remedy the breach, including engaging a new IT vendor and hiring the services of a data protection consultant.

39. In view of the factors noted above, the Commission has decided not to issue any direction to either Challenger or Xirlynx to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning to Challenger and Xirlynx respectively for the breach of their respective obligations under section 24 of the PDPA.

40. The Commission emphasises that it takes a very serious view of any instance of non-compliance with 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
COMMISSION MEMBER
PERSONAL DATA PROTECTION COMMISSION

[1] See section 2(1) of the PDPA.
[2] See section 2(1) of the PDPA.
[3] See section 2(1) of the PDPA.