DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1512-A613

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 (the "PDPA")

And

Propnex Realty Pte Ltd (UEN No. 199903004H)

… Organisation

Decision Citation: [2017] SGPDPC 1

GROUNDS OF DECISION

25 January 2017

A. BACKGROUND

1. On 28 December 2015, the Personal Data Protection Commission ("**Commission**") received a complaint from the Complainant in relation to the publication online of the Organisation's internal Do Not Call list containing the personal data of 1765 individuals, including the Complainant and her sisters ("**PropNex DNC List**"). Following the Complainant's complaint, the Commission undertook an investigation into the matter. The Commission's grounds of decision are set out below.

2. The Complainant alleged that she and her sisters had been receiving marketing calls and messages from various telemarketers (including moneylenders) on their mobile telephone numbers even though they had not consented to being contacted.

3. When the Complainant spoke to one of the telemarketers over the phone to ask where he had obtained her telephone number, she was informed that her name and telephone number were available on the Internet. This prompted the Complainant to conduct a search on the Internet for her name. Among the search results was a URL link ("**Link**") to the PropNex DNC List dated 29 July 2015 in PDF format.

4. The PropNex DNC List contained, amongst other things, the Complainant's full name, mobile number and landline, residential address and internal instructions to the Organisation agents regarding the Complainant.

B. MATERIAL FACTS AND DOCUMENTS

5. The Organisation is a real estate agency. P&N Holdings Pte Ltd ("**P&N Holdings**") is the parent company of the Organisation. Investigations disclosed that P&N Holdings and the Organisation share a common IT infrastructure. P&N Holdings maintains and operates the common IT infrastructure and provides IT support to the Organisation.

6. On 28 December 2015, the Commission was informed that the personal data of the 1,765 individuals contained in the PropNex DNC List was accessible to the public through the Link (the "**Data Breach Incident**"). PropNex DNC List was accessible to the public without authentication either through the Link or by performing an online search using search terms, for example, the Complainant's name, "PropNex" or the phrase "user files do not call". Investigations disclosed that the PropNex DNC List was disseminated internally as a PDF file that was uploaded onto the Organisation Virtual Office System ("**VO System**"). For reasons detailed below, this PDF file was searchable and accessible on the Internet.

7. The PropNex DNC List included the following personal data:

   (a) name;

   (b) mobile number and/or landline;

   (c) full or partial residential address;

   (d) date of complaint by a particular individual;

   (e) email address; and

   (f) internal instructions by the Organisation to its agents with regard to the individuals.

8. The Commission estimates that 96% or more of the records in the PropNex DNC List only contained a telephone number, residential address or email address without any other identifying information.

9. On 31 December 2015, the Commission informed the Organisation's Data Protection Officer of the Data Breach Incident and requested that the PropNex DNC List be taken down. The Organisation confirmed that the PropNex DNC List belongs to the Organisation and that it had no knowledge of the Data Breach Incident until it was notified of the complaint. On 4 January 2016, the Organisation deleted the PropNex DNC List from its VO System and informed Google to exclude the Link from its search results. The Organisation also took steps to prevent a re-occurrence of the Data Breach Incident, by introducing a new way of disseminating the DNC List internally through a secured database and which can be searched using an authenticated web form.

10. Investigations disclosed that in or around July 2015, the PropNex DNC List was in PDF format and placed in a shared folder for internal use on the VO System which was accessible only by the Organisation agents and staff through authenticated login. Earlier versions of the PropNex DNC List had been placed in the same shared folder since the beginning of 2015.

11. The Organisation represented that it had put in place data protection policies, which were made known to its employees through briefings and addendums to their employment agreements. The Organisation also submitted that it had carried out penetration tests for its IT systems, and performed periodic searches on Google for possible leaked documents. In addition, the Organisation conducted security testing for web applications such as the VO System whenever major changes were conducted, and used "/robots.txt" to hide documents from Google's search engine crawler as well as to provide another layer of security for documents stored in the VO System.

12. However, the Organisation admitted that there was no password security whatsoever for the PropNex DNC List. The VO System's authentication only worked for web pages and not documents such as PDF files, which was the intended design and limitation of the original system. In relation to the shared folder in the VO System, this was meant for forms and templates and not "sensitive documents", but this policy was neither formally recorded nor communicated to users. Over time, therefore, this design limitation remained as a vulnerability but was overlooked.

13. According to the joint investigation carried out by the Organisation and P&N Holding, the Data Breach Incident was found to have occurred because the PropNex DNC List was indexed by Google and was therefore searchable and available on the Internet. This occurred despite the fact that the PropNex DNC List was stored in a restricted web folder. This case demonstrates the weakness of relying on "/robots.txt" to hide the documents from the Google search engine crawler.

C. COMMISSION'S FINDINGS AND ASSESSMENT

14. At the outset, the Commission considers that the PropNex DNC List, containing amongst other things, individuals' names, contact numbers, residential addresses and email addresses, does constitute personal data as defined in Section 2(1) of the Personal Data Protection Act 2012 ("**PDPA**"). In addition, the Commission notes that the PropNex DNC List was an internal list maintained and stored on the Organisation's VO System. The Organisation does not dispute that the personal data in the PropNex DNC List contained personal data under the control of the Organisation at the material time.

15. Under Section 24 of the PDPA, an organisation is obliged 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 ("**Protection Obligation**").

16. Accordingly, pursuant to Section 24 of the PDPA, the Organisation is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to or of the PropNex DNC List.

Relationship between the Organisation and P&N Holdings and their obligations under the PDPA

17. Investigations disclosed that even though P&N Holdings and the Organisation shared a common IT infrastructure, with P&N Holdings maintaining and operating the common IT infrastructure and providing IT support to the Organisation, there was no evidence to suggest that P&N Holdings processed any personal data on behalf of the Organisation. Accordingly, the Commission does not consider that P&N Holdings is a data intermediary of the Organisation.

Adequacy of Security Arrangements

18. After carefully considering all the relevant facts and representations made by the Organisation, the Commission is of the view that the Organisation failed to take reasonable security measures to protect the personal data in its possession and/or under its control. The Commission's reasons are set out below.

19. First, based on the Commission's investigations into the matter, the Commission finds that the VO System contained a significant system weakness, namely, that user authentication was only applied to webpages (e.g. aspx files) but was not in place for document files (e.g. PDF files). As a result of this weakness in the VO System, any user could have direct access to document files on the VO System, including the PropNex DNC List, by typing the Link in an Internet browser or through a Google search without having to go through any form of user authentication.

20. The Organisation was aware of this system weakness and it recognised that as a result of this system weakness, sensitive documents should not be placed on the VO System. However, the Organisation did not implement any security arrangements to militate against this known system weakness. For example, there was no policy to prohibit the sharing of sensitive documents on the VO System or to require that sensitive documents shared on the VO System be protected by a password.

21. Consequently, the PropNex DNC List was placed on the VO System as a PDF file without any password security or authentication, which in turn allowed the Data Breach Incident to occur and allowed various

telemarketers to access and make use of the personal data in the PropNex DNC List.

22. Second, the Organisation's approach towards protecting the documents in the VO System through the use of "/robots.txt" was not sufficient and evinced an incorrect or inadequate understanding of the security measure which they chose to implement. The Organisation used "/robots.txt" in an attempt to hide the documents from the Google search engine crawler. The Organisation intended for this to be another layer of security for the documents stored in the VO System.

23. However, there are recognised weaknesses and limitations to relying on "/robots.txt" to hide the documents from the Google search engine crawler. For example, non-compliant (e.g. malicious) web crawlers might ignore the instructions in a "/robots.txt" file. The Organisation claims that it had only discovered these weaknesses and limitations after the Data Breach Incident. Contrary to the Organisation's claims, these weaknesses and limitations of "/robots.txt" are referred to in introductory articles such as the Google support article, "*Block URLs with robots.txt; Learn about robots.txt files*", which is easily accessible. The Organisation referred to this article in its representations, thereby showing that the Organisation could have and should have been aware of these weaknesses and limitations when they made use of this security measure.

24. The "/robots.txt" script was implemented to hide the webpages in the VO System from search engine crawlers; however, it cannot restrict or prevent access by external parties. Simply hiding a link to a document on the world wide web is not an effective way of ensuring that the document itself is protected from unauthorised access. The fact is that the document is still available online, and can be accessed by anyone over the world wide web. If the intent was to ensure that the document was for internal use, then appropriate restrictions and security measures should be placed to limit access to only the authorised persons.

25. Each organisation should adopt security arrangements that are reasonable and appropriate in the circumstances. If an organisation decides to use a particular security measure, it should be responsible for understanding the weaknesses and limitations (if any) of such a measure and to design and shape its security arrangements in light of those weaknesses and limitations.

26. It remains for the Commission to observe that the Organisation had implemented security arrangements and conducted periodic security testing. However, the Commission is of the view that the security arrangements and testing undertaken by the Organisation were insufficient to militate against the weaknesses in the VO System and to protect the personal data stored on the system. The technical limitations discussed above demonstrate this. Additionally, the Organisation had failed to discover the breach for a period that could extend to five (5)

months, from the time the PropNex DNC List was first placed in the VO System until a complaint was brought against it. This reinforces the Commission's finding that the security arrangements that had been implemented were insufficient to deter or to detect a data breach.

27. The Commission further finds that the corrective measures taken by the Organisation after the Data Breach Incident are only sufficient as an interim measure. Specifically, the Commission notes that following the Data Breach Incident, the Organisation had removed the PropNex DNC List from the VO System, and shifted it to a database which was accessible only through a new web application which required user authentication. However, the Organisation did not put in place any user authentication for document files stored in the VO System. Consequently, there is a risk that the Organisation's agents could continue to place unprotected document files containing personal data in the VO System, which would expose such personal data to the same risks as those arising from the Data Breach Incident, which could potentially result in other data breaches.

Exceptions under the Fourth Schedule of the PDPA

28. In its representations, the Organisation had indicated that it was relying on exceptions in paragraphs 1(a) and (h) of the Fourth Schedule of the PDPA. However, the Organisation did not explain how the foregoing exceptions would apply in respect of the Protection Obligation. Nonetheless, the Commission considered the potential application of these exceptions. In its deliberations, it was not apparent how the Organisation's disclosure of the PropNex DNC List "*is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way*"[1] or "*is necessary for evaluative purposes*".[2] Accordingly, the Commission considers that the Organisation's reliance on the exceptions to the Consent Obligation in paragraphs 1(a) and (h) of the Fourth Schedule of the PDPA is irrelevant to this case, and without merit.

D. ENFORCEMENT ACTION BY THE COMMISSION

29. Having completed its investigation and assessment of this matter, the Commission finds that in light of the weakness in the VO System and the failure to implement security arrangements which would militate against the known VO System weaknesses, the Organisation failed to take reasonable security measures to protect the personal data in its possession and/or under its control and is in breach of Section 24 of the PDPA.

30. 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$10,000 be imposed on the Organisation.

31. During the course of investigations, the Organisation represented that the VO System was not intended to be used for the storage or sharing of documents containing personal data. However, the Commission notes that the VO System is a system that is meant for the online sharing of documents between the Organisation agents and/or employees through the Internet. This being the case, it is foreseeable that some of the documents stored and/or shared on this system may contain personal data. The Commission there additionally directs that the Organisation:

(a) ceases the storage and/or sharing of documents containing personal data using the VO System until the design flaw of the VO System has been fixed; and

(b) conducts a security scan on the VO System to identify and fix any additional vulnerabilities before it is made accessible online.

32. In assessing the breach and the directions to be imposed, the Commission took into account the following factors:

(a) the Data Breach Incident involved 1,765 individuals and their personal data was disclosed to the public;

(b) the Data Breach Incident was caused by a flaw in the Organisation's VO System;

(c) The Organisation admitted to the Data Breach Incident in the first instance;

(d) 96% or more of the records concerning the 1,756 individuals contained either a telephone number, residential address or email address without any other personal data;

(e) The Organisation took prompt remedial actions to rectify and prevent the recurrence of the data breach;

(f) The Organisation had been cooperative and forthcoming during the investigations;

(g) The Organisation did have in place a data protection policy which they made known to their agents and staff; and

(h) The Organisation's in-house compliance team (with the assistance of external consultants, where necessary) did conduct annual internal audits to assess:

(i) system access risk;

(ii) data integrity risk; and

(iii) risk of configuration issues in production environment.

33. 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

---

[1] Paragraph 1(a) of the Fourth Schedule of the PDPA.
[2] Paragraph 1(h) of Fourth Schedule of the PDPA.