PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPCS 5

Case No. DP-2212-C0526

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

And

Century Evergreen Private Limited

SUMMARY OF THE DECISION

1. On 11 December 2022, the Personal Data Protection Commission (the **"Commission"**) received a complaint against Century Evergreen Private Limited (the "**Organisation**") that images of identification documents (which includes the National Registration Identity Card) submitted by jobseekers to the Organisation were publicly accessible on the Organisation's website ("**Incident**"). The Organisation is a manpower contracting services company and required jobseekers to submit their identification documents to verify the identity of and suitability of the jobseeker in question.

2. Following the complaint received, the Commission commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**"). The Organisation requested that the investigation be handled under the Commission's Expedited Decision Procedure ("**EDP**"). This means that

the Organisation voluntarily provided and admitted to the facts set out in this decision. The Organisation also admitted that it failed to implement reasonable security arrangements to protect the personal data in its possession and control, and was in breach of section 24(a) of the PDPA.

3. The Organisation admitted that the Insecure Direct Object References ("**IDOR**") vulnerability on its website, which allowed the complainant to manipulate the URL had existed from the time the website was launched on 9 November 2015. As a result of this vulnerability, 96,889 images of identification documents belonging to 23,940 individuals were downloaded from the Organisation's website from 10 to 12 December 2022.

4. The Organisation admitted that it was in breach of section 24(a) of the PDPA as it failed to include any security requirements to protect personal data in its contract with the vendor who first developed and subsequently maintained the website. In this regard, even though the Organisation had engaged an IT vendor from the time the website was developed and launched, the Organisation remained solely responsible for protecting the personal data in its possession and control at all material times.

5. What is expected from organisations who engage professional services to build their websites and other online portals is explained in the Commission's Guide on Building Websites for SMEs (revised 10 July 2018) (the "**Guide**"). The Commission had consistently advised organisations of the need to emphasise the protection of

personal data to their IT vendors, by making it part of their contractual terms.[1] The contract should clearly state the responsibilities of the IT vendor with respect to the PDPA. In this regard, the Commission noted that there was a glaring omission of clauses to protect personal data in the Organisation's contract with its IT vendor.

6. The Organisation also admitted that apart from conducting functionality testing when the website was first launched, the Organisation had no arrangements with its IT vendor to conduct any security tests prior to the launch of the website, or thereafter. The Organisation had also failed to impose any security requirements on the IT vendor to protect personal data, via contract.

7. In view of the above, the Deputy Commissioner found that the Organisation had contravened section 24(a) of the PDPA.

8. In deciding the appropriate outcome in this case, the Commission considered that a financial penalty ought to be imposed as the personal data affected included not just the identification numbers, but the images of the identification documents. Furthermore, there was a long period of non-compliance. The vulnerability was not addressed since 2015.

9. In deciding on the appropriate amount of financial penalty, the circumstances set out above and the factors listed at section 48J(6) of the PDPA were considered, specifically the impact of the personal data breach on the individuals affected and the nature of the Organisation's non-compliance with the PDPA. In the circumstances, this was not an insignificant breach given the number of individuals

[1] See Guide on Building Websites for SMEs (revised 10 July 2018) at [4.2.1] and Re EU Holidays Pte Ltd [2019] SGPDPC 38.

affected (ie 23,940) and the nature of personal data exfiltrated: 96,889 images of identification documents.

10. The Organisation's non-compliance with the PDPA was also not simply one of mere negligence but that of gross negligence. There was a long period of non-compliance on the facts of this case. As set out above, the Commission had issued the Guide to assist SMEs, and consistently cautioned the need for organisations to ensure compliance with the PDPA even when they engage an IT vendor in our previous decisions.[2]

11. In deciding on the appropriate amount of the financial penalty, the following factors were considered – the Organisation's turnover and profitability, its cooperation throughout the investigation, its voluntary admission of breach of the Protection Obligation under the EDP, and the prompt remedial actions taken after the Organisation became aware of the IDOR vulnerability. This included rectifying the IDOR vulnerability, making server configuration changes to improve security, implementing vulnerability scans, migrating its backup server to an encrypted remote server, deploying additional security software and subscription to security services, and securing a new contract with its vendor to manage the security of its website. In addition to its prompt remedial actions, its poor performance in the most recent financial year was also taken into consideration. Finally, the organisation had admitted to its culpability at an early stage and elected to proceed under the EDP.

[2] Re EU Holidays Pte Ltd [2019] SGPDPC 38 and Re Vhive Pte Ltd (Case No. DP-2013-B8138).

12. For the reasons above, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$9,000 within 30 days from the notice accompanying date of this decision, failing which interest at the rate specified in the Rules of Court in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

The following section of the Personal Data Protection Act 2012 had been cited in the above summary:

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 –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.