PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 17

Case No DP-1802-B1674

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

And

InfoCorp Technologies Pte. Ltd.

… *Organisation*

DECISION

InfoCorp Technologies Pte. Ltd.

Tan Kiat How, Commissioner — Case No DP-1802-B1674

20 June 2019

Background

1 The case concerns the unauthorised access and disclosure of personal data arising from a registration exercise for a crypto-currency initial coin offering ("**ICO**"). The Personal Data Protection Commission ("**PDPC**") received six complaints on the matter on 5 February 2018. The Organisation also notified the PDPC of the matter on the same day.

2 Following an investigation into the matter, the Commissioner found the Organisation in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**"). The Commissioner's findings and grounds of decision of the matter are set out below.

Material Facts

3 The Organisation had conducted a crypto-currency ICO registration exercise via a website[1] ("**Website**") which it owned and managed at the material time. The registration exercise was scheduled to take place between 5 and 26 February 2018.

---

[1] https://sentinel-chain.org/.

4 The registration process involved two main parts.

(a) Individuals ("**Participants**") were asked to input name, email address, date of birth, identification type and number, nationality, country of residence and residential address ("**Personal Data Set**") on the registration page.

(b) Participants also had to upload Know-Your-Customer ("**KYC**") documents. A Uniform Resource Locator ("**URL**") would be assigned to a Participant after he or she had uploaded the KYC documents and clicked "Save". The KYC documents included the following:

i. An identification document with a photograph of the Participant;

ii. Documents showing proof of residence; and

iii. A photograph of the Participant holding the identification document.

5 The incident was caused by a vulnerability in the design of the registration form. There was no requirement built into the system to authenticate the individuals downloading the KYC documents. The URL also contained a serialised file identity ("**FileID**") as the last few characters of the URL in running numbers. The vulnerability allowed Participants assigned with a URL to access other Participants' saved KYC documents by altering the last few characters of the assigned URL. The KYC documents of 21 Participants were downloaded by 15 other Participants via this vulnerability.

6 The Organisation took the server offline immediately after being informed by a Participant. The Organisation also contacted the 15 other

Participants who had downloaded the KYC documents. They were told to destroy the KYC documents not belonging to them. This includes any personal data of other Participants that they may have retained.

7 Prior to the incident, the Organisation had engaged a vendor to design the registration form for the Website. Data protection elements were considered by the Organisation. The Personal Data Sets were to be encrypted and rendered inaccessible to third parties. Nonetheless, the same level of diligence with respect to the uploaded KYC documents was not exercised by the Organisation.

8 The Organisation conducted standard functional tests on the Website's process and user flow prior to launching it. However, these did not detect the vulnerability that caused the incident. The Organisation also did not conduct nor arrange for any penetration test or web application vulnerability scan.

The Commissioner's Findings and Basis for Determination

9 The issue for determination is whether the Organisation breached section 24 of the PDPA. Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

10 The Organisation had full possession and control over the personal data collected from the Participants. Although the Organisation had engaged a vendor to design the registration form, the vendor did not process any personal data on behalf of the Organisation. The Organisation managed the Website on its own. Thus, it retained full responsibility for the IT security of the Website and the personal data contained therein.

11 The Commissioner is satisfied that reasonable security arrangements had been made to protect the Personal Data Sets despite the vulnerability. Encryption of the Personal Data Sets had prevented unauthorised access by third parties.

12 However, insufficient protection was accorded to the KYC documents. The Organisation had only performed standard functional tests of the Website prior to launching it. No penetration test or web application vulnerability scan was conducted. Had these tests and scans been performed on the Website, the well-known vulnerability could be easily detected.

13 Given the type of personal data that the KYC documents contained, it is unreasonable that the Organisation had omitted the abovementioned security testing prior to the Website launch. The ease with which the vulnerability could be exploited via changing the last few numbers of the URL made this more egregious.

14 The Commissioner therefore finds the Organisation in breach of section 24 of the PDPA.

The Commissioner's Directions

15 Given the Commissioner's findings that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

16 In assessing the breach and determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account the following mitigating factors:

(a) The URL was only known to Participants at the material time and not to the public.

(b) The KYC documents were only downloaded by a small number of Participants.

(c) The exposure was for a very short time window of about 15 minutes.

(d) The Organisation had taken immediate remedial actions to prevent further unauthorised access of the KYC documents.

(e) The Organisation was cooperative during the investigation.

(f) The Organisation had promptly notified the PDPC of the incident.

17 The Commissioner hereby directs the Organisation to pay a financial penalty of S$6,000 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[2] in respect of judgement debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

---

[2] Cap 322, R5, 2014 Rev Ed.