i-vic International Pte. Ltd.

[2019] SGPDPC 41

Yeong Zee Kin, Deputy Commissioner — Case No. DP-1804-B1991

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

12 November 2019.

Introduction

1 The Employment and Employability Institute Ltd ("**e2i**") administers a work trial programme on behalf of a public agency, Workforce Singapore ("**WSG**"). e2i engaged i-vic International Pte Ltd (the "**Organisation**") to process claims and queries from members of the public relating to the work trial programme (the "**Engagement**").

2 On 16 April 2018, e2i reported to the Personal Data Protection Commission (the **"Commission"**) that documents containing personal data of three individuals (the "**Affected Individuals**") involved in the work trial programme were inadvertently attached to emails sent out by the Organisation to 9 individuals (the "**Incident**").

Material Facts

3 As part of the Engagement, the Organisation was required to manage e2i's mailbox which received emails from members of the public with their claims and queries. It was also required to develop and/or maintain the IT infrastructure and customer relationship

management (“**CRM**”) software (collectively, the “**System**”) used to operate and manage e2i’s mailbox. As part of this, the Organisation was required to either reply to the emails from members of the public (providing the appropriate responses) or escalate the queries in the emails to the relevant e2i representatives. Where an email query needed to be escalated, an employee of the Organisation would submit an escalation request in the System. The System would then automatically generate two emails for the Organisation’s employee to send (the “**Automated Email Generation Process**”). The first was a holding reply email to the person who had sent the email query to e2i’s mailbox and the second was an email to escalate the query to the relevant e2i representative. For the second email, the System would automatically retrieve the relevant documents that were stored in the Organisation’s servers and attach them to the email.

4 On the 1st of every month, the Organisation ran a batch process on the System, after normal working hours, to generate reward programme emails for an another client (the “**Reward Programme Process**”). While this was being done, the Automated Email Generation Process was unable to run any instructions to generate and send emails. During this time, any instructions by the Organisation’s employees to generate emails with respect to the Engagement would be queued and the Automated Email Generation Process would process these instructions as a batch once the Reward Programme Process had been completed.

5 On 1 April 2019, while the Reward Programme Process was being run, one of the Organisation’s employees attempted to generate some new emails using the Automated Email Generation Process. These instructions to generate the relevant emails were queued, to be acted upon only after the Reward Program Process was completed. However, due to an error in the

Automated Email Generation Process code for processing emails as a batch, the System attached the wrong documents containing personal data of the Affected Individuals to the emails in the queue and sent these out to 9 different individuals.

6 The documents that were sent to the 9 individuals contained the names, NRIC numbers, signatures, residential addresses, mobile numbers, email addressed, age and race of all three Affected Individuals, the bank account number of two of the Affected Individuals and the highest academic qualifications, work trial company details and work experience details of one of the Affected Individuals (collectively referred to as the "**Disclosed Personal Data**").

Remedial actions by the Organisation

7 After becoming aware of the Incident, the Organisation took the following remedial action to prevent it from reoccurring:

(a) Fixed the error in the code of the Backlog Clearing Process which caused the Incident; and

(b) Rewrote the relevant code to enable automated encryption of attachments (so that unauthorised recipients would not be able to view the contents of the attachments) and to ensure that the wrong files would not be attached to emails.

Findings and Basis for Determination

8 Section 24 of the PDPA provides that 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 (the "**Protection Obligation**").

9 As a preliminary point, it is noted that e2i was acting on behalf of WSG in relation to the collection, use and disclosure of personal data for administration of the work trial programme. As such, pursuant to section 4(1)(c) of the PDPA, e2i was not subject to Part III to VI of the PDPA, including section 24, in relation to such collection, use and disclosure of personal data.

10 The Organisation was a data intermediary of e2i as it processed personal data on behalf of e2i for the purpose of the Engagement. The Organisation was thus required to protect personal data in its possession or under its control in accordance with section 24.

11 In relation to the cause of the Incident, the Organisation asserted that it had tested the code of the Automated Email Generation Process. However, the Organisation also admitted that it had not tested how the code acted when the Automated Email Generation Process processed instructions to generate and send emails which were queued while the Reward Programme Process was running. In this regard, the Organisation explained that they expected such emails to be processed and sent out individually and not queued while the Reward Programme Process was running. Nevertheless, as the Organisation ought to have known that the Automated Email Generation Process was unable to run while the Reward Programme Process was running on the 1st of every month, the Organisation ought to have tested whether

this had an effect on the Automated Email Generation Process. Diligent and properly scoped testing would have simulated the circumstances leading to the Incident and would therefore likely have detected that documents containing personal data were being incorrectly attached to the emails in queue.

12 In the circumstances, the Organisation's failure to put in place diligent and properly scoped testing amounted to a failure to put in place reasonable security arrangements to protect the personal data which was in its possession and/or under its control. I therefore find that the Organisation had contravened section 24 of the PDPA.

The Deputy Commissioner's Directions

13 In view of the above findings, I hereby direct the Organisation to pay a financial penalty of $6,000 within 30 days from the date of this direction, failing which, interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

14 I have decided not to issue any further directions as the Organisation has taken the actions set out at paragraph 7 above to remedy the cause of the Incident.