WRITTEN VOLUNTARY UNDERTAKING ("Undertaking")
TO THE PERSONAL DATA PROTECTION COMMISSION

This Undertaking is given to the Personal Data Protection Commission or its delegates pursuant to section 48L(1) of the PDPA, by:

Employment and Employability Pte. Ltd.
UEN: 200704772C
Registered Address: 30 Cecil Street, #19-08, Prudential Tower,
Singapore 049712

(hereinafter referred to as the "**Organisation**").

By signing this Undertaking, the above-named Organisation acknowledges the matters stated herein and undertakes to the Commission in the terms set out herein.

1. DEFINITIONS

1.1 In this Undertaking:

(a) "**PDPA**" means the Personal Data Protection Act 2012 (No. 26 of 2012); and

(b) "**Relevant Provisions**" means the provisions in Parts III, IV, V, VI, VIA and IX, and section 48B(1) of the PDPA.

2. ACKNOWLEDGEMENTS

2.1 The Organisation hereby acknowledges the following matters:

(a) The Commission has carried out investigations into certain acts and practices of the Organisation, and has reason to believe that the Organisation has not complied, is not complying, or is likely not to comply with one or more of the Relevant Provisions. The relevant facts and circumstances are summarised at Schedule A.

(b) As a result of any non-compliance with the PDPA by an organisation, the Commission has a number of enforcement options under the PDPA,

including the option to issue directions under sections 48I or 48J of the PDPA.

(c) The Commission recognises that the Organisation has made efforts to address the concerns raised in this case and to improve its personal data protection practices. In addition, the Organisation was cooperative in the course of the investigation and was responsive to requests for information. The Commission further recognises that the Organisation appears ready to implement or is in the midst of implementing the steps set out in Schedule B.

(d) Having carefully considered all the relevant facts and circumstances, the Commission takes the view that this is an appropriate case in which an Undertaking may be accepted.

2.2 The Organisation also acknowledges and agrees that the Commission may publish and make publicly available this Undertaking, and without limitation to the foregoing, the Commission may issue public statements referring to this Undertaking and/or its contents in whole or in part.

3. UNDERTAKINGS

3.1 The Organisation undertakes that it has taken, or will take all necessary steps, to carry out the actions or refrain from carrying out the actions referred to in Schedule B, and where applicable, in accordance with the stipulated timelines.

4. COMMENCEMENT

4.1 This Undertaking shall take effect upon the acceptance by the Commission of the Organisation's duly executed Undertaking.

5. THE COMMISSION'S STATUTORY POWERS

5.1 In order to provide the Organisation with an opportunity to complete all necessary steps to implement its undertakings set out in clause 3 above, the Commission will exercise its powers under section 50(3)(ca) of the PDPA to suspend the investigations referred to in clause 2 on the date the Undertaking takes effect as set out in clause 4.1.

5.2 The Organisation acknowledges that the Commission will verify the Organisation's compliance with its undertakings set out in clause 3 above, and

if necessary, will exercise its powers under the Ninth Schedule of the PDPA to do so.

5.3 Clause 5.1 above shall be without prejudice to the Commission's statutory powers to conduct or resume, at any time, the investigations referred to in clause 2 above if it thinks fit, including but not limited to the situation where the Organisation fails to comply with this Undertaking or part thereof in relation to any matter.

5.4 Nothing in this Undertaking, including the Commission's acceptance of the Undertaking, is intended to, or shall, fetter or constrain the Commission's rights and statutory powers (including but not limited to those under sections 48I, 48J, 48L(4) and 50 of the PDPA) in any manner. Neither shall be construed as creating any anticipation or expectation that the Commission will take or not take any particular course of action in the future (whether in the present case or in respect of any other case concerning a breach or suspected breach of the PDPA). The acceptance of this Undertaking is strictly confined to the particular facts of the present case, and is made on the basis of the representations and information provided by the Organisation. The acceptance of an Undertaking in this case shall not be construed as establishing any precedent.

6. VARIATION

6.1 This Undertaking may be varied only with the express written agreement of the Commission.

This document has been electronically signed. The Parties hereby affirm that the electronic signatures have been affixed with the due authorisation of each Party and that Parties intend for the electronic signatures to carry the same weight, effect and meaning as hand-signed wet-ink signatures.

SIGNED, for and on behalf of)

Employment and Employability Institute Pte. Ltd.)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

ACCEPTED by)

)

Name: _____)

Designation: Deputy Commissioner

Personal Data Protection)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

DP-2106-B8424

1. On 2 June 2021, the PDPC received feedback of a personal data breach incident by Employment and Employability Institute Pte. Ltd. ("**e2i**"). When an individual registers for a course, talk or event organised by e2i on e2i's website, the website would automatically populate and display an individual's personal data once an individual's NRIC number is inserted into the website. If an individual uses the person's NRIC number on e2i's website, there would be the risk of unauthorised disclosure of personal data by e2i if such use had not been duly authorised.

2. As a result, the personal data of 102,151 individuals' was at risk of a potential personal data breach. The types of personal data affected included the following:
   i) Name
   ii) Citizenship
   iii) Union member status
   iv) Gender
   v) Race
   vi) Highest education level
   vii) Unemployed since
   viii) Unemployment duration (months)
   ix) Reason for unemployment
   x) Education level detail (field of study, qualification name/title, institution, date of completion)
   xi) Work experience (From, to, company name, industry, job title, job duties, masked last drawn salary/month)
   xii) Background and health (Ex-offender, bankruptcy, color blindness, medical illness, drug abuse)
   xiii) Partially masked NRIC
   xiv) Partially masked date of birth
   xv) Partially masked email address
   xvi) Partially masked postal code
   xvii) Partially masked contact number (Home/HP)

3. The PDPC notes that there was no evidence of exfiltration of the personal data.

DP-2103-B8132

1. On 25 March 2021, the PDPC received a data breach notification from e2i, which involved its outsourced contact centre, i-vic International Pte. Ltd. ("**i-vic**"). Personal data from 2 email accounts of an i-vic employee was downloaded by a malicious actor. It was found that i-vic had put in place reasonable security arrangements despite the data breach.

2. However, it was found that e2i had failed to stipulate reasonable data protection requirements when selecting i-vic as its data intermediary, and in its contract with i-vic. It was also found that e2i lacked sufficiently robust processes to protect personal data during transmission. There were at least 18 occasions where e2i's employees had sent large volumes of personal data to i-vic without protection.

3. The personal data of 31,002 individuals' was downloaded by a malicious actor in the incident. The types of personal data affected included the following:
   i) NRIC
   ii) Partial NRIC Number
   iii) Date of Birth
   iv) Mobile Number
   v) Landline
   vi) Email Address
   vii) Residential Address
   viii) Highest Qualification
   ix) Employment Details – containing salary, employment status, occupation or company name

SCHEDULE B

REMEDIATION PLAN

A. **In Progress**

S/N	Remedial Steps/Measures	How does this measure address the issue	Target Completion date	Status
1	**Strengthen e2i's data protection governance** e2i will appoint an independent vendor to conduct a professional review of our organisation's data protection practices through a comprehensive health check. The scope of engagement will include: • Assessment of our existing data protection policies and practices, and recommend solutions to close gaps; • Conduct a table-top exercise to test the data breach response plan; • Managing our data intermediaries by putting in place governance and risk assessment; policies and practices; service management, and exit management. After the above review has been implemented, the vendor will continue to review our data protection policies and practices through regular health checks. This will enable us to continually	This will ensure our Data Protection Management Programme (DPMP) is relevant and optimised for operations and continuous improvements: • Data collected is adequate, relevant and limited to what is necessary and processed with the intended purpose. • Ensure appropriate controls are in place to secure data and procedures in place for staff to recognise and respond to potential data breach incidences. • Ensure there is a framework and process	16 Feb 2023 - we are looking at a 1-year timeframe to complete the exercise with the following breakdown: 4 months: Confirming review specifications and appointment of an independent vendor to assess our existing policies, guidelines, and SOPs. Interview business units to identify relevant work processes and gaps. 5 months: Review and implement recommendations to bridge all gaps. Conduct	In progress

	identify and address risks and gaps and implement solutions to close them.	to govern our data intermediaries	table-top exercise to test data breach response plan. 3 months: Produce reports on the reviews and table top exercises that were carried out. Setup proactive monitoring such as regular audit period and inspection exercises for our practices and data intermediaries.	

2	**Professional IT security review and tightening of vendor selection process** e2i has engaged a professional company to conduct IT Risk Assessment Audits on third-party vendors to ensure our vendors have the necessary cybersecurity frameworks and systems in place for data protection. Criteria(s) are put in place to tighten our vendor selection process. This ensures that the vendor has frameworks and procedures in place to manage and protect data, such as its storage security and access rights by different types of users; how does the vendor ensure compliance with PDPA such as training of staff and the IT system's robustness.	This will ensure better governance on our third-party vendors' IT security and data protection capability.	Jun 2022	In progress

3	**OTP Implementation on e2i's website** Option 1 To implement an authentication (via OTP) interface before an individual reached the personal data confirmation page using the current Events Management SystHem ("EMS") Option 2 As current EMS is due for renewal or change by Oct 2022, e2i may explore a new EMS. In this case, e2i will implement the OTP on the new EMS. However, this means e2i will need a longer timeline as e2i has to evaluate different vendors and the functionalities the vendors can offer.	With the OTP, users will have the added protection of their personal data from being accessed by anyone using their NRIC number	Option 1: Mar 2022 Option 2: Oct 2022	In progress. e2i will review whether to renew contract with current vendor or explore a new EMS and update PDPC on its decision of implementing Option 1 or Option 2 by Mar 2022. In the meantime, information has been masked such that only the user's partially masked contact number is left, which is not identifiable.

B. **Implemented**

S/N	Remedial Steps/Measures	How does this measure address the issue	Timeframe	Status
1	**IT and personal data handling checks on Call Centre vendors** **For i-vic International (Contract ended 31 Aug 2021):** • All i-vic staff supporting e2i's work are using company-issued desktops and laptops. No unmanaged devices, including mobiles, are used for e2i's work. • Implementation of multi-factor authentication to all user accounts supporting e2i's work and scanning all staffs' laptops to ensure no further incidence of malware • Advisory to i-vic to adopt different modes of communication for sharing of passwords. **For new call centre Agape Connecting People Pte Ltd (Contract started from 1 September 2021)** Checks were made to ensure they had: • Secured data management system	To prevent further unauthorised access and ensure that our call centre has the necessary IT systems and processes in place to protect our personal data.	March 2021 (for i-vic) September 2021 (for Agape due to change in vendor)	Completed

	• Safer mail software (Microsoft 365 with 2-factor enabled password authentication) • Secured data centre (Managed offsite at Telin, ISO certified vendor (ISO/IEC 27001:2013) • Secured network server (Lantone Systems, housed locally, same company serving SingTel) • 24/7 IT systems monitoring • Overall enhancement in data sharing methods between vendor and e2i • Quarterly review on IT systems			
2	**Tightened vendor selection process** Current and future third-party vendors dealing with personal data to complete an Information Security Third-party assessment questionnaire to understand their processes on capturing personal data, IT security controls, and compliance. Incorporate legal clauses on PDPA data management in current and future contracts with vendors	To ensure better governance on our third-party vendors' IT security and data protection capability.	From April 2021	Completed
3	**Enhancement to password protection policy** In addition to previous password policies, we required all newly changed system access passwords to be 12 characters long, comprising English letters with at least one upper case, numbers and special characters.	To enhance policies and SOPs set in place to guide staff on the password management for systems and documents containing personal information.	May 2021	Completed

	Staff were also reminded to adhere to password guidelines: i. Staff should send password using a different channel; ii. Staff should set password that are unique, unpredictable and changed on a regular basis			
4	**Enhanced outlook system security** e2i has implemented the following system security: • Secure Web Gateway and Data Leak Prevention solutions in e2i laptop • Data Loss Prevention feature to protect sensitive information in Microsoft O365 environment • Implemented Geo-location restriction for Microsoft O365 accounts	This ensures that IT solutions are in place to prevent personal data leakage.	May to July 2021	Completed

5	**Continuous effort to conduct regular PDPA and cybersecurity awareness training and to share good cybersecurity practices with employees.** • All new staff (including temps) need to complete an e-learning module on PDPA 101 within their 1st week of joining and before they handle personal data • Yearly PDPA workshop for all staff • Advisory emails sent to staff to remind them about good PDPA and cybersecurity practices • Organisation-wide meetings feature a segment on good PDPA practices, reminders on PDPA governance • Internal meetings (Risk/Management meetings) – PDPA compliance is regularly highlighted and addressed.	Staff are equipped with PDPA knowledge and adequate competencies to comply with our SOPs and policies.	On-going	Completed

6	**Masking of personal information on e2i's registration page** To implement the masking of personal data within the Events Management System registration confirmation page, only leaving the user's partially masked contact number within the user interface. The individual needs to only verify event details they have signed up for.	This will avoid any user using another NRIC number to access another person's personal data after registration for an event due to the auto-population feature	October 2021	Completed

TrustedData PowersInnovation
10 Pasir Panjang Road, #03-01, Mapletree Business City, Singapore 117438
t. (65) 6377 3131 | f. (65) 6577 3888 | www.pdpc.gov.sg