**PERSONAL DATA PROTECTION COMMISSION**

**[2019] SGPDPC 29**

Case No DP-1805-B2112

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

And

Friends Provident International Limited

… *Organisation*

---

**DECISION**

---

# Friends Provident International Limited

Yeong Zee Kin, Deputy Commissioner – Case No. DP-1805-B2112

30 July 2019

**Facts of this Case**

1 Friends Provident International Limited is a company established in the Isle of Man which provides life assurance services in Singapore through a registered branch office (the "**Organisation**"). In the course of providing these services, it operates and maintains an online portal (the "**Portal**") through which its policyholders can request for changes to their particulars, for example, contact details. On 10 May 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving the disclosure of certain personal data of policyholders obtained from the Portal. The circumstances leading to the incident were as follows.

2 The Organisation's policyholders and certain other authorised personnel could access the Portal via a "Secured Mailbox" webpage on the Organisation's website (the "**Secured Mailbox Webpage**"). Policyholders could, as noted above, submit certain requests via the Portal and the Organisation's authorised personnel accessed the Portal in order to process these requests. For this purpose, the Organisation's authorised personnel could generate reports containing the data of policyholders who had made a request ("**Reports**"). These Reports were stored in the Portal and could be obtained thereafter by the Organisation's authorised personnel.

3 The ability to generate and obtain Reports from the Portal was intended to be restricted to the Organisation's authorised personnel. To achieve this, when a user logged in to the Secured Mailbox Webpage, the system would determine whether the user was one of the Organisation's authorised personnel or a policyholder. If the user was one of the authorised personnel, a 'Report' tab would be displayed in the Secured Mailbox Webpage which enabled the authorised personnel to generate and obtain Reports. The 'Report' tab was hidden from the view of policyholders when they accessed the Secured Mailbox Webpage. Apart from hiding the 'Report' tab, no additional or separate authorisation was necessary in order to generate and obtain Reports from the Portal and there was no subsequent verification (after the user logged in) as to whether the user was, in fact, authorised to generate and obtain the Reports via the 'Report' tab.

4 As a result of a faulty JavaScript within the Secured Mailbox Webpage, the 'Report' tab was visible to policyholders when they re-sized their desktop internet browser to a smaller size or if they accessed the Secured Mailbox Webpage via a mobile device. As no verification or separate authorisation was required to access the 'Report' tab and generate and obtain Reports, such policyholders were able to generate and obtain Reports from the Portal once the 'Report' tab was visible (collectively referred to as the "**Vulnerability**").

5 The exploitability of the Vulnerability, which had likely existed since 30 September 2017 when the Secured Mailbox Webpage was introduced, was fortuitously resolved on 6 February 2018 when the Secured Mailbox Webpage was enhanced and backend verification was included. Unfortunately, on 12 December 2017, one of the Organisation's policyholders discovered that he could generate and obtain Reports from the Portal that contained the names, policy numbers and regions of residence of other policyholders. He subsequently reported this to the Monetary Authority of Singapore which, in turn, notified the Organisation of the incident

(the "**Reported Breach**"). The Organisation had been unaware of the Vulnerability until they were notified of the Reported Breach.

6 The Organisation subsequently determined that before the Vulnerability was fixed, 42 Reports had been produced and downloaded by 21 policyholders or their advisors. The total number of individuals affected by this was estimated to be 240, 11 of whom had their policy numbers disclosed. After the Reported Breach, the Organisation undertook the following as part of its remedial actions:

(a) reviewed the Portal to ensure that the Reports were no longer accessible by unauthorised personnel;

(b) conducted an initial risk assessment and commenced an immediate investigation into the Reported Breach;

(c) imposed a requirement that regression testing must be conducted for mobile devices and different screen resolutions;

(d) ensured that backend access validation was in place on top of front-end validation;

(e) ensured that all employees received training on data protection upon commencement of employment, which would be refreshed annually; and

(f) contacted the policyholder who had generated and downloaded Reports on 12 December 2017 to ensure that he no longer held the Reports that he downloaded.

**Findings and Basis for Determination**

7 Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**") requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, disclosure and similar risks. I find that the Organisation had not done so, and is in breach of section 24, for two main reasons: first, the manner in which the Organisation restricted access to the Reports was insufficient to prevent unauthorised access to the Reports and the personal data they contained and, secondly, the testing of the Secured Mailbox Webpage was inadequate.

8 On the first point, what is most striking in this case is the lack of an authorisation mechanism for access to the ability to generate and obtain Reports. Once a user gained access to the Secured Mailbox Webpage and could view the 'Report' tab (in the circumstances noted above), no further authorisation or verification was required to generate and obtain Reports from the Portal via the 'Report' tab. The only means the Organisation employed to limit access to the Reports was to hide the 'Report' tab from the view of unauthorised persons. This was insufficient as there could be various ways in which the hidden tab could be revealed, even without the faulty JavaScript, such as by manipulating the scripts or widgets running on the Secured Mailbox Webpage.

9 On the second point, given that the Secured Mailbox Webpage was intended for use across a variety of devices and screens, testing should have been conducted across multiple browsers and devices. While organisations are not expected to test across all possible browsers and devices, testing should have been done on representative devices (in the present case, with different screen or browser sizes) based on the design and intended functionality of the Secured Mailbox Webpage. The Organisation's failure to do so meant that its testing was ultimately inadequate to address the risk of unauthorised access to the personal data in the Reports. In

fact, simply accessing the Secured Mailbox Webpage on a mobile device as part of its tests would have revealed the Vulnerability to the Organisation. Additionally, organisations and developers should note that the testing of other browser conditions such as script blocking, while not mandatory, is highly recommended. In the Organisation's case, script blocking would also have caused the 'Report' tab to become visible.

**Outcome**

10 Taking the totality of the circumstances into account, I have decided to issue a warning to the Organisation for its contravention of section 24 of the PDPA. In reaching this conclusion, I note that:

(a) the potential for misuse of the personal data disclosed was relatively low because the data was not of a nature where identity theft could be committed; and

(b) the Organisation had promptly notified the Commission and implemented remedial actions upon learning of the Reported Breach.

**YEONG ZEE KIN**
**DEPUTY COMMISSIONER**
**PERSONAL DATA PROTECTION**