DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1603-A656

GMM TECHNOWORLD PTE. LTD.
(UEN. 201103748R)

... Respondent

Decision Citation: [2016] SGPDPC 18

GROUNDS OF DECISION

30 September 2016

A. BACKGROUND

1. GMM Technoworld Pte. Ltd. (the "**Respondent**") is a small and medium enterprise (SME) retailing products such as waterproof gadgets and measuring instruments. In particular, the Respondent is the sole distributor of DiCAPac, a brand of waterproof cases for cameras and mobile phones.

2. On 3 March 2016, the Personal Data Protection Commission (the "**Commission**") received a complaint from a member of public regarding the alleged disclosure of personal data on the Respondent's corporate website at http://www.dicapac.com.sg/frm_display/product-warranty-registration/ (the "**Webpage**").

3. The Commission decided to carry out an investigation into the matter and its findings are set out below.

B. MATERIAL FACTS AND DOCUMENTS

4. The Respondent created a corporate website (www.dicapac.com.sg) on a WordPress platform for the purpose of marketing its products. The website was hosted on a third party server and comprised several publicly accessible webpages. In 2014, the Respondent added a product warranty registration feature to the website at http://www.dicapac.com.sg/product-warranty-registration-form/ (the "**Warranty tab**").

5. The Warranty tab contained an online warranty registration form (the "**Form**") for customers who purchased a DiCAPac waterproof case to register for the product warranty. This Form was created using Formidable Forms, a third-party

paid plug-in for WordPress, which allowed for the capture of personal data on the website (the "**Plug-in**"). The information to be provided in the Form included the customers' names, email addresses, mobile phone numbers and residential addresses.

6. The Plug-in had the function of dynamically listing and displaying on the Webpage the personal data that was collected on the website via the Plug-in. According to the Respondent, it was unaware of this function of the Plug-in, and had thought that the personal data that was collected was only viewable by the administrator of the website. As a result of the Respondent's misunderstanding of the functionality of the Plug-in and the (incorrect) use of the Plug-in, the personal data of approximately 190 individuals collected through the Plug-in was displayed on the Webpage, which was publicly accessible on the Internet.

7. After being notified of the breach, the Respondent undertook certain corrective actions to rectify the unauthorised disclosure.

C. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Relevant issue in this case

8. Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") states that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised disclosure, disposal, access, collection, use, or similar risks (amongst others).

9. The relevant issue in this case is whether the Respondent had in place reasonable security arrangements to protect the personal data in its possession or in its control, as required under section 24 of the PDPA.

Commission's findings on the relevant issue

10. In this case, the Commission found that the Respondent was ignorant of or unaware that one of the functions of the Plug-in was to display the personal data collected on the website. Further, the Commission found no reasonable excuse for the Respondent's ignorance for the following reasons.

11. First, the Plug-in was promoted on the Formidable Forms website with the following description indicative of its functions "[d]on't just collect information, display it".[1] Second, the product documentation webpage contained the

[1] Excerpt from Formidable Forms website (https://formidablepro.com/).

following statement "[a]ny data entered into a Formidable Form can be displayed on your site using Views".[2] On the same webpage, one of the display options under the heading "View Format" was "All Entries", which was described as an option that would "[l]ist all entries from the specified form".[3] Third, the Formidable Forms website had a 'demos' webpage that allowed users to try out or download a demonstration of how the information captured by the Plug-in would be displayed. In gist, a dominant feature of the Plug-in is that it provided online form functionalities for the collection *and display* of information on the web site.

12. In this regard, the Formidable Forms website had webpages which provided adequate demonstrations, documentation and explanations of its products, including the Plug-in, accompanied by pictorial guides. In the Commission's view, an organisation ought to have sufficient understanding and appreciation of a product before making use of it. In this case, had the organisation studied these sources, it would have become aware that use of the Plug-in would result in the disclosure of the data collected on the website since the Plug-in was designed to ease the collection and display of information. For the organisation's purpose of collecting but not displaying personal data, the default behaviour of the out-of-the-box features of this Plug-in would not be appropriate. Alternatives could have been considered. If alternatives are not suitable and the organisation decides to proceed with using the Plug-in, it should be responsible for understanding the security features offered by the Plug-in and it would have to set the security features accordingly. It would not be prudent for an organisation to use a plug-in without first being clear of the default behaviour of its functions in relation to the collection of personal data, and without ensuring that the plug-in (if properly configured) adequately protects the organisation's personal data.

13. For completeness, investigations revealed that the Respondent did not mention taking any further steps to protect the personal data in its possession or under its control. Instead, the Respondent appears to have relied on the belief that the paid Plug-in itself was sufficiently secure out-of-the-box.

14. Ultimately, the Respondent's lack of awareness of the Plug-in's actual functions, its wrong use of the Plug-in, and failure to take steps to configure it appropriately led to the unauthorised disclosure of the personal data of approximately190 individuals. Accordingly, this was a breach of section 24 of the PDPA.

---

[2] Excerpt from Documentation of Formidable Forms "View Settings" (https://formidablepro.com/knowledgebase/display-your-form-data/).
[3] Excerpt from Documentation of Formidable Forms "View Settings" (https://formidablepro.com/knowledgebase/display-your-form-data/).

D. THE COMMISSION'S DIRECTIONS

15. The Commission is empowered under section 29 of the PDPA to give the Respondent such directions as it deems fit to ensure the Respondent's compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding S$1 million as the Commission thinks fit.

16. In determining whether a direction should be given to the Respondent in this case, the Commission has given due consideration to all the relevant factors, including the following:

    (a) the Respondent was cooperative and provided its responses to the Commission on a timely basis; and

    (b) the Respondent took immediate steps to stop the further unauthorised disclosure, and implemented corrective measures to protect its customers' personal data.

17. Pursuant to section 29(2) of the PDPA, and having completed its investigation and assessment of this matter, the Commission is satisfied that the Respondent was in breach of the protection obligation under section 24 of the PDPA.

18. Having carefully considered all the relevant factors of this case, the Commission hereby directs the Respondent to pay a financial penalty of S$3,000 within 30 days from the date of the Commission's direction, failing which interest shall be payable on the outstanding amount of such financial penalty.

19. The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION