PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 1

Case No DP-1903-B3441

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

And

Iapps Pte Ltd.

… *Organisation*

DECISION

Iapps Pte Ltd

[2021] SGPDPC 1

Lew Chuen Hong, Commissioner — Case No DP-1903-B3441

10 February 2021

Introduction

1 On 1 March 2019, the Personal Data Protection Commission (the "**Commission**") received a complaint from an individual (the "**Complainant**") in relation to potential unauthorised disclosure of his personal data through the ActiveSG mobile application (the "**ActiveSG App**"). The Complainant's concerns arose because he was able to view another individual's personal data when he logged into his child's supplementary account on the ActiveSG App (the "**Incident**")

Facts of the Case

2 ActiveSG is a national movement for sports coordinated by Sport Singapore,[1] a statutory board of the Ministry of Culture, Community and Youth. Iapps Pte Ltd (the "**Organisation**") is a financial technology company specialising in mobile application development and marketing. Sport Singapore engaged the Organisation to develop, deploy and operate the Super Sports Club Membership Management System ("**SSCMMS**"). The functions of SSCMMS included membership registration, and the ActiveSG App was a component of

[1] Sport Singapore was formerly known as Singapore Sports Council.

the SSCMMS. Members of ActiveSG could use the ActiveSG App to book sport facilities, register for fitness classes and purchase entry passes to ActiveSG sport centres.

3 Sport Singapore is the owner of the SSCMMS and ActiveSG App. Pursuant to the written contract between the Organisation and Sport Singapore, the Organisation's scope of work included providing and operating the production server for the ActiveSG app. The Organisation also developed, deployed and operated the SSCMMS (including the ActiveSG App).

4 On 1 March 2019, the Organisation's engineer developed a security code fix for the ActiveSG App. The security code fix was meant to be deployed into the enterprise environment (which was a test environment) for further testing. However, due to human error, the security code fix was deployed into the production environment, resulting in the Incident.

5 According to the Organisation, the personal data of 153 individuals (the "**At Risk Individuals**") had been at risk of unauthorised access by 84 individuals during the Incident. Out of the At Risk Individuals, there was actual unauthorised access of 108 individuals' (including 9 minors below the age of 18) (the "**Affected Individuals**") names and NRIC numbers ("**Disclosed Data**") by 84 individuals who were able to view this information when logging into their own accounts on the ActiveSG App. For 6 of the Affected Individuals, in addition to the Disclosed Data, there was also actual unauthorised access of additional personal data, including (collectively, the "**Additional Disclosed Data**"):

(a) Email address;

(b) Mobile telephone number;

(c) Home telephone number;

(d) Address;

(e) Gender;

(f) Date of birth;

(g) Race;

(h) Employment status; and

(i) Sports Interests.

6 Upon being notified of the Incident on the same day, the Organisation immediately took the following remedial actions:

(a) Rectified the issue within 2 hours of the Incident;

(b) Reminded its staff to be careful and vigilant in the course of their work; and

(c) Together with Sport Singapore, implemented the following measures:

(i) Separated the enterprise environment and production environment that were previously on the same server;

(ii) Put in place 2-factor authentication for the Organisation's engineers to access the production environment. This means that the engineers are required to obtain the 2-factor one-time password from Sport Singapore to access the production environment;

(iii) Monitoring of affected users for suspicious activities; and

(iv) Implemented dynamic QR codes for member IDs.

7 Sport Singapore also notified the Affected Individuals about the Incident.

The Commissioner's Findings and Basis for Determination

8 There is the preliminary issue of whether the Organisation was a data intermediary for Sport Singapore, and whether it could avail itself of the exception under the previous section 4(1)(c) of the of the Personal Data Protection Act 2012 ("**PDPA**").[2]

9 Effective 1 February 2021, the exclusion in section 4(1)(c) of the PDPA has been amended to be limited to "public agencies" only. Organisations acting on behalf of public agencies in relation to the collection, use or disclosure of public data (even when in an agency relationship of the type described below), are now subject to obligations under the PDPA, and cannot claim to be excluded from the same.

10 As the Incident in this case occurred prior to 1 February 2021, the applicability of the exclusion under the previous section 4(1)(c) of the PDPA remains to be considered. However, the Commission makes clear that this exclusion will not be applicable or considered in future cases.

---

[2] Prior to 1 February 2021, section 4(1)(c) of the PDPA provided that "any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data is not subject to the obligations under Parts III to VI of the PDPA"

11 The exclusion in the previous section 4(1)(c) of the PDPA for organisations acting on behalf of public agencies was based on the legal concept of agency i.e. where the organisation was authorised by a public agency to act in its place, as its agent, and the agent manifested assent or otherwise consented to so act.[3] Whether an agency relationship was created in any particular case is essentially a question of fact. Relevant factors to take into consideration when determining whether an agency relationship arose included the communications between the parties and their conduct, as well as the terms of any relevant contract.

12 The underlying question in each case was whether the organisation was authorised to act on behalf of the principal. The authorisation by the principal in an agency relationship is usually made expressly, although it could in some cases be by implication from the conduct or situation of the parties. Where there is such authority, the acts of the agent that are within the scope of the authority are the acts of the principal, which would be legally liable for the acts of its agent.[4]

13 In the present case, the Commission's investigations revealed that the Organisation was at all material times an independent third party vendor. There was nothing in the contract between the parties which expressly authorised the Organisation to act on behalf of Sport Singapore. The clauses in the contract pointed to the Organisation being a service provider to Sport Singapore, and not its agent. Further, there was an indemnity clause in the contract which obliged the Organisation to among others, indemnify and keep Sport Singapore fully

---

[3] See *Alwie Handoyo v Tjong Very Sumitomo and anor* [2013] 4 SLR 308 at [147]

[4] See *Ong Han Ling and anor v American International Assurance Co Ltd and ors* [2018] 5 SLR 549 at [208]

indemnified against all actions, claims, demands, losses, expenses arising out of or in connection with the performance of the contract by the Organisation. As explained at [11] – [12], if the Organisation and Sport Singapore were in an agency relationship, acts of the agent (i.e. the Organisation) within the scope of authority would be acts of the principal (i.e. Sport Singapore) who would be legally liable for acts of its agent. An indemnity would therefore not be necessary. The presence of the indemnity clause is evidence that the relationship was not a principal-agent relationship. In addition, Sport Singapore confirmed that it had never appointed the Organisation to act in its place. In the circumstances, the exclusion in the previous section 4(1)(c) of the PDPA did not apply to the Organisation.

14 With respect to whether the Organisation was acting as a data intermediary, the Commission's investigations found that the Organisation was engaged to carry out activities of "processing" personal data on behalf of Sport Singapore as defined in section 2(1) of the PDPA. As mentioned at [3], the Organisation's scope of work included developing, deploying and operating the SSCMMS (including the ActiveSG App). In the course of operating the SSCMMS and the ActiveSG App, the Organisation organised and retrieved the Disclosed Data and the Additional Disclosed Data on the behalf of Sport Singapore. In addition, the Organisation also processed service requests (which included enquiries and extraction of information including the Disclosed Data and Additional Disclosed Data) on behalf of Sport Singapore. The Organisation was therefore acting as a data intermediary of Sport Singapore

Whether the Organisation had contravened section 24 of the PDPA

15 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 or similar risks.

16 The obligation to make reasonable security arrangements does not attach unless an organisation was in possession or control of personal data. In the present case, the Organisation provided the production environment and operated the SSCMMS (including the ActiveSG App). The Organisation therefore had actual possession of the Disclosed Data and Additional Disclosed Data and control of the processing activities that they had contracted to provide. Therefore, prior to the Incident, they were obliged to put in place reasonable security arrangements to protect the Disclosed Data and Additional Disclosed Data.

17 The Commission's investigations revealed that the Organisation's processes for the deployment of code into production and test environments were not sufficiently robust to safeguard against risks of deployment of codes into the wrong environment.

(a) According to the Organisation, its usual code deployment process went through 3 stages (i) User Acceptance Testing ("**UAT**"); (ii) "enterprise environment" (i.e. test environment); and (iii) production environment.

(b) Due to human error on the part of its engineer, the Organisation's processes and procedures for the deployment of the security code fix into the ActiveSG App were not followed. After the UAT was completed, the code that was meant to be deployed to the testing environment was instead deployed directly into the production environment. This is a grave and serious error with, as is evident in this case, potentially severe consequences. In this regard, the Commission's

investigations revealed that the Organisation did not have second-level approvals or supervisory checks in its processes for the deployment of codes into the test environment. This meant there was no oversight of the code deployment process nor any supervision of the actions of the Organisation's engineers after UAT was completed.

(c) As stated in the Commission's previous decisions, relying solely on employees to perform their duties diligently is not a sufficient reasonable security arrangement – organisations should take practical steps to implement its policies and procedures to protect personal data, including identifying areas of high risk that require higher level of approval and adequate supervision.[5] In the present case, the deployment of the security code fix into the ActiveSG App could potentially expose the Disclosed Data and the Additional Disclosed Data to security risks. The Organisation should have identified this risk, and implemented a second-level check to ensure that its engineers deployed the codes into the correct environment. Alternatively, the Organisation could have automated its processes by using development operations software that would automate the correct deployment of code.

(d) The absence of any second-level checks in the Organisation's processes for the deployment of codes and lack of any other form of security arrangement to safeguard against risks of deployment of codes into the wrong environment amounted to weak internal work process controls.

---

[5] See *Re Aviva Ltd* [2017] SGPDPC 14 and *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34

18 For the reasons above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

19 After being notified of the Commission's proposed decision including the proposed financial penalty amount, the Organisation made representations to the Commission suggesting that (i) the Organisation had done the necessary to comply with section 24 of the PDPA, or (ii) that a warning ought to be administered in lieu of the Commission's proposed financial penalty. The Organisation's representations were rejected for the following reasons:

(a) The Organisation contended that it *did* have second-level checks for the deployment of code, and referred the Commission to its Standard Operating Procedure ("**SOP**") for the SSCMMS. While the SOP did describe multi-level checks at the UAT stage (i.e. the *first* stage of testing), it not dictate any second-level checks relating to the deployment of code into the enterprise environment, and thereafter production environment (i.e. the second and third stages). In fact, the SOP contained *no* references to deployment of code in the enterprise environment at all. The Organisation failed to provide any evidence of any second-level checks after UAT and before deployment of the code in production.

(b) The Organisation claimed that the Incident was the result of human error which happened "*in the rush of the moment*" and would not have been prevented by a second level check. The Commission disagrees. For the reasons stated at 17(c) and 17(d) above, the appropriate processes such as a second-level check or automated code deployment via software should have been implemented, and would have prevented the Incident. Such processes are all the more necessary

considering the time pressure that engineers often operate under, as appears to have happened in this case.

(c) The Organisation highlighted that it had taken prompt remedial actions after discovery of the Incident (listed at [6] above). The Commission accepts that the remedial action taken by the Organisation was timely and sufficient. This has been taken this into consideration in quantifying the financial penalty imposed in this case (as set out below), and in deciding that no further directions need be issued to the Organisation.

Financial Penalty

20 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the Commissioner took into account the factors listed at section 48(6) of the PDPA, including that:

(a) that the Disclosed Data included the NRIC numbers of 9 minors;

(b) The Organisation cooperated with the Commission's investigations; and

(c) The Organisation implemented prompt remedial actions (i.e. the issue was fixed within 2 hours of the Incident).

21 On 23 July 2020, the Organisation was given notice of the Commission's intention to impose a financial penalty of S$11,000 and was invited to make representations. Having considered the Organisation's representations dated 21 August 2020, 21 October 2020, and 29 October 2020,

as well as all the relevant factors of this case, the Commissioner hereby requires the Organisation to:

(a) pay a financial penalty of S$9,000 within 30 days from the date of the notice accompanying this decision, 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 the financial penalty until it is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION