Grabcar Pte Ltd

[2020] SGPDPC 14

Yeong Zee Kin, Deputy Commissioner — Case No. DP-1909-B4675

Data Protection – Protection obligation – Unauthorised access to personal data – Insufficient security arrangements

21 July 2020

Introduction

1 Grabcar Pte Ltd (the "**Organisation**") is a Singapore-based company offering ride-hailing transport services, food delivery and digital payment solutions through its mobile application (the "**Grab App**"). The Grab App also provides a carpooling option referred to as "GrabHitch". GrabHitch matches a passenger with a driver willing to give a lift to the passenger (on the way to the driver's destination) in return for a fee. On 30 August 2019, the Organisation notified the Personal Data Protection Commission (the "**Commission**") that, for a short period of time on the same day, profile data of 5,651 GrabHitch drivers was exposed to the risk of unauthorised access by other GrabHitch drivers through the Grab App (the "**Incident**").

Facts of the Case

2 The Organisation's investigations traced the cause of the Incident to the deployment of an update to the Grab App on 30 August 2019 (the "**Update**"). The purpose of the Update was to address a potential vulnerability discovered within the Grab App, namely, the application programming interface ("**API**") endpoint (/users/{userID}/profile) (the "**URL**") that had allowed GrabHitch drivers to access their data, contained a 'userID' that could potentially be manipulated to allow access to other GrabHitch driver's data.[1]

3 In order to fix the vulnerability, the Update removed the variable 'userID' from the URL which shortened it to a hard-coded '/users/profile'. However, the Update failed to take into account the URL-based caching mechanism in the Grab App. This caching mechanism (which was configured to refresh every 10 seconds) served cached content in response to data requests to reduce the load of direct access to the Organisation's database.

4 With the deployment of the Update, all URLs in the Grab App ended with "/users/profile". Without the variable 'userID' in the URL (which directed data requests to the correct GrabHitch driver's accounts), the caching

[1] According to the Organisation, there was no evidence that this vulnerability had been exploited.

mechanism could no longer differentiate between GrabHitch drivers. Consequentially, the caching mechanism provided the same data to all GrabHitch drivers for 10 seconds before new data was retrieved from the Organisation's database and cached for the next 10 seconds.

5 As a result of the Incident, a total of 21,541 GrabHitch drivers' and passengers data was exposed to the risk of unauthorised access (collectively "**Personal Data Sets**"):

(a) Profile pictures;

(b) Passenger names;

(c) Vehicle plate number; and

(d) Wallet balance comprising journal history of ride payments.

6 In addition to the Personal Data Sets, other data that was exposed to the risk of unauthorised access during the Incident included GrabHitch booking details such as addresses and pickup and drop-off times; and driver details such as total rides, vehicle model and make.

7 Upon being notified of the Incident, the Organisation took the following remedial actions:

(a) Rolled back the Grab App to the version prior to the Update within approximately 40 minutes;

(b) Notified 5,651 GrabHitch drivers of the Incident on the same day; [2]

(c) Increased the minimum "cash out" amount for wallets in GrabHitch to S$200,000 to prevent unauthorised transfers;

(d) Deployed a new update for the Grab App on 10 September 2019;

(e) Reviewed its testing procedures including implementing mandatory automated tests for all API endpoints dealing with personal data;

(f) Updated governance procedures concerning deployment and security verification on changes to IT systems and applications; and

[2] The Organisation's initial investigations indicated that 5,651 GrabHitch drivers' data was exposed to the risk of unauthorised access due to the Incident. Following further investigations, the Organisation determined that up to 21,541 GrabHitch drivers' and passengers data was exposed to the risk of unauthorised access.

(g) Embarked on an architecture review of its legacy applications, and relevant codes which had not been reviewed for an extended period of time.

The Commissioner's Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

8 Section 24 of the Personal Data Protection Act 2012 ("**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. It is not disputed that the Organisation had possession and control of the Personal Data Sets at the material time.

9 In the context of the present case, given that the Organisation made changes to its IT system that processed the Personal Data Sets, it is obliged to put in place reasonable security arrangements to prevent any compromise to the Personal Data Sets.[3] The Organisation failed to do so for the reasons explained below.

[3] *Re Flight Raja Travels Singapore Pte Ltd* [2018] SGPDPC 16 at [8].

10 First, the Organisation did not put in place sufficiently robust processes to manage changes to its IT system that may put the personal data it was processing at risk. This was a particularly grave error given that this is the second time the Organisation is making a similar mistake, albeit with respect to a different system.[4]

(a) The Organisation introduced changes to the Grab App (through the Update) without understanding how the changes would operate with existing features of the Grab App and its broader IT system, including the caching mechanism.

(b) In particular, the Update involved changes to the URL (i.e. removing the variable 'userID'). The variable 'userID' in the URL had the function of ensuring that data requests (including the Personal Data Sets) were directed to the correct GrabHitch drivers' accounts. However, the Organisation implemented the Update without making an assessment whether the Grab App would continue to direct data requests to the correct GrabHitch drivers' accounts without the variable 'userID' in the URL.

---

[4] See *Re Grabcar Pte Ltd* [2019] SGPDPC 15 at [17] where it was found that the Organisation did not have adequate measures in place to detect whether the changes it made to a system that held personal data introduced errors that put the personal data it was processing at risk.

11 Second, the Organisation did not conduct properly scoped testing before the Update to the Grab App was deployed.

(a) As found in the Commission's previous decisions, organisations are obliged to conduct properly scoped testing before new IT features or changes to IT systems are deployed. These tests need to mimic real world usage, including foreseeable scenarios in a normal operating environment when the changes are introduced.[5] Such tests prior to deployment are critical to enable organisations to detect and rectify errors in the new IT features and/or be alerted to any unintended effects from changes that may put personal data at risk.[6]

(b) In the present case, the Organisation admitted that it did not conduct tests to simulate multiple users accessing the Grab App, whether concurrently or consecutively. The Organisation also admitted that it did not conduct any specific test to verify how the caching mechanism would work in tandem with the Update.

---

[5] *Re AIA Singapore Pte Limited* [2019] SGPDPC 20 at [15] and *L'Oreal Singapore Pte. Ltd.* Case No. DP 1812-B3091, Summary of the Decision at [3].

[6] See for example *Re Flight Raja Travels Singapore Pte Ltd* [2018] SGPDPC 16 and *Re Singapore Telecommunications Limited* [2019] SGPDPC 36.

(c) In view of the large number of GrabHitch drivers, multiple users logging in concurrently or consecutively are foreseeable scenarios that the Organisation should have simulated during its testing of the Update prior to deployment. Properly scoped pre-launch tests would have included an assessment of how the caching mechanism may affect the intended operation of the Update because the caching mechanism can affect data requests returned to the GrabHitch drivers.

12 For the reasons above, I find the Organisation in breach of section 24 of the PDPA.

The Deputy Commissioner's Directions

13 In determining the directions, if any, to be imposed on the Organisation under Section 29 of the PDPA, I took into account as a mitigating factor that the Organisation cooperated with the investigation, and was prompt and forthcoming in its response to queries during the Commission's investigations. I have also taken into consideration that this is the fourth time the Organisation has been found in breach of Section 24 of the PDPA.[7] Given that the

[7] The previous decisions being *Re Grabcar Pte Ltd* [2018] SGPDPC 23; *Re Grabcar Pte Ltd* [2019] SGPDPC 14; and *Re Grabcar Pte Ltd* [2019] SGPDPC 15.

Organisation's business involves processing large volumes of personal data on a daily basis, this is a significant cause for concern.

14 Having considered all the relevant factors of this case, I direct the Organisation to pay a financial penalty of S$10,000 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 the financial penalty until it is paid in full. In order to reduce the risk of another data breach, I also direct the Organisation to put in place a data protection by design policy for its mobile applications within 120 days of the date of this direction.
