GrabCar Pte. Ltd.

[2018] SGPDPC 23

Tan Kiat How, Commissioner — Case No DP-1706-B0871

Data Protection – Protection obligation – Disclosure of personal data - Insufficient security arrangements

Data Protection – Personal Data – Business contact information

27 September 2018.

Background

1 This case involves the unauthorised disclosure of the personal data of GrabHitch drivers in a Google Forms survey created by the Organisation that was accessible online (the "**Incident**"). The Personal Data Protection Commission (the "**Commission**") received a complaint from one of the drivers whose personal data was disclosed in the Incident and commenced its investigations thereafter. The Commissioner set out below his findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

2 The Organisation was incorporated in September 2014 and has been providing the GrabHitch service since November 2015. GrabHitch is a paid carpooling service operated by the Organisation that matches individual non-commercial private car owners ("**Hitch Drivers**") with people who are

commuting along the same route.[1] Hitch Drivers are permitted to charge a fare to cover the Hitch Driver's variable costs, such as petrol and car depreciation based on the distance of the ride.

3 In accordance with the Organisation's Driver's Code of Conduct, Hitch Drivers who fail to comply with the Terms and Conditions or Code of Conduct may be penalised through account deactivation, the withholding, reduction or forfeit of driver incentives or credits, suspension or permanent banning. Conduct that would warrant a suspension of a Hitch Driver's account include fraud, booking and cancellation offences, offences concerning fares and payments and passenger experience, safety or security offences such as harassment.

4 At the time of the Incident, the Organisation had suspended the accounts of 20 Hitch Drivers for various offences such as unacceptable behaviour and/or usage of the platform; these Hitch Drivers had appealed their suspensions. Of these 20 Hitch Drivers, two of them were also GrabCar drivers. The Organisation created the "GrabHitch SG Appeal Form" using Google Forms, to allow the Hitch Drivers to submit an appeal to the Organisation and for the Organisation to contact them for further investigation.

5 Hitch Drivers whose accounts had been suspended were able to access the Google Form on 16 June 2017 at 10am. They were required to fill up the following fields in the Google Form ("**Appeal Form Data**") if they wanted to submit an appeal to the Organisation:

---

1 Individuals who provide carpool trips that adhere strictly to the conditions set out in the Road Traffic (Car Pools) (Exemption) Order 2015 are exempt from the certain requirements under the Road Traffic Act (Cap. 276), such as the requirement to obtain the appropriate commercial licences and insurance.

(a) Name as per NRIC;

(b) NRIC number;

(c) Mobile number;

(d) Vehicle Plate; and

(e) Appeal Statement to explain their case for appeal including reasons to justify the reactivation of their account.

6 The Incident was the first time that the Organisation used Google Forms for the purposes of collecting responses in respect of appeals. Its intention was to allow its employees to access and review the Appeal Form Data to review suspensions. However, the employee who was responsible for uploading the Google Form had chosen the incorrect setting by selecting the setting "*Respondents can: See summary charts and text responses*". As a result, all Hitch Drivers who had submitted the Google Form to appeal their suspensions were able to view all the Appeal Form Data contained in the responses, both their own as well as the other Hitch Drivers who had appealed. Investigations disclosed that only the Hitch Drivers and the Organisation's employees were able to access the Appeal Form Data.

7 After being notified of the Incident, the Organisation promptly removed the ability of Hitch Drivers to access the Appeal Form Data. The total duration that the Google Form was in use was less than 8 hours; the Appeal Form Data was uploaded on the same morning that the complaint was received and access to the data by Hitch Drivers was removed by 5pm the same day.

Findings and Basis for Determination

8 The issues for determination are:

(a) whether the information disclosed constituted personal data; and

(b) whether the Organisation breached section 24 of the PDPA.

9 Even though it was an employee of the Organisation who had uploaded the Google Form with the wrong settings, under section 53(1) of the PDPA, any act done or conduct engaged in by a person in the course of his employment shall be treated for the purposes of the PDPA as done or engaged in by his employer as well as by him, regardless of whether it was done or engaged in with the employer's knowledge or approval. The Organisation is therefore responsible for its employee's conduct in relation to the Incident.

Whether the information disclosed constituted personal data

10 In this case, given that individual Hitch Drivers can be identified from the Appeal Form Data which was disclosed in the Incident (specifically, the Hitch Drivers' names, mobile phone numbers, NRIC numbers, vehicle plate numbers as well as their appeal statements), the Appeal Form Data is personal data as defined in the PDPA. In this regard, the Organisation is required to comply with the data protection obligations under the PDPA in respect of the Appeal Form Data.

11 Also, the Organisation in its representations dated 14 May 2018 indicated that the suspensions or bans were in relation to Hitch Drivers allegedly either exceeding the statutorily allowed number of trips per day or to "game" the system. The Organisation has subsequently, on 1 June 2018, in response to

a question from the Commission on why the Organisation treated such transgressions as worthy of a suspension, stated that:

> We take gaming very seriously as it affects the integrity of our service offerings. Also, it is against our driver Code of Conduct: https://www.grab.com/sg/driver/hitch/code-of-conduct/. I draw your attention to the following clauses:
>
> Provide an honest service. Any form of cheating (e.g. Failure to return the full balance to passengers or requesting for full payments during promotional periods) or suspected fraudulent activity is prohibited and will trigger further investigation from the Company, as we reserve the right to ensure all transactions are genuine.
>
> The Company maintains a zero-tolerance policy regarding all infringements and violations of this Code of Conduct and the Driver acknowledges that this may result in suspension or termination of user access to the Grab platform

12 It is therefore the Organisation's case that a driver who "games" the system exhibits a lack of probity suggestive of fraudulent intent. These are serious allegations and the Organisation ought to have treated such personal data with the appropriate care in the knowledge that the unauthorised disclosure of the Appeal Form Data would result in such serious allegations being disclosed as well.

13 As noted at paragraph 4 above, two out of the 20 Hitch Drivers are also drivers of GrabCar. In this regard, unlike GrabHitch, which is a non-commercial social carpooling service, GrabCar is a private-hire car service that allows passengers to book a chauffeured ride for a fee and can only be provided by vehicles and drivers with the appropriate commercial licences. There is therefore the additional consideration that, pursuant to section 4(5) of the PDPA, the data protection obligations do not apply to business contact information of these two GrabCar drivers. (Business contact information is defined to be an

individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.)

14 In *Re Comfort Transportation Pte Ltd and another* [2016] SGPDPC 17 ("***Comfort Transportation***") (at [9]), the Commissioner found that taxi drivers' mobile phone numbers that were used for, or related to, their business as taxi drivers fell within the definition of "business contact information" because, among other things, the organisation disclosed the taxi drivers' mobile phone numbers to passengers as a means for them to contact the taxi driver after a booking has been made. Thus, the name and mobile phone numbers provided by the two GrabCar drivers who were also Hitch Drivers are considered business contact information. The vehicle plate number is not business contact information since this is a means of *identification of the vehicle* that was used to provide the commercial GrabCar service and the driver of the said vehicle, but not a means of *contacting the driver*. That said, their NRIC numbers would not fall within the definition of business contact information.

Whether the Organisation breached section 24 of the PDPA

15 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Organisation represented that it uses the Single Sign-On authentication process with Google's suite of authentication services to protect access to the Appeal Form Data. Access to the Appeal Form Data is accessible only to intended individuals through individual file sharing permissions.

16 However, as mentioned above, the Incident had occurred because the employee responsible for uploading the Google Form had chosen the incorrect setting "*Respondents can: See summary charts and text responses*". At the time of the Incident, the Organisation did not have any policies or procedures to guide their employees regarding the use of Google Forms to collect personal data nor did it provide any training. Following from the Incident, the Organisation represented in its response to the first Notice to Produce dated 11 July 2017, that it was in the midst of preparing documents to better guide their employees on the use of Google Forms to prevent a similar occurrence in the future.

17 The Incident was the first time that Google Forms were used for the purposes of collecting responses (including the Hitch Drivers' personal data) in respect of appeals. Since there are easily accessible introductory articles such as the Google support article "*What can you do with Forms*?",[2] the onus is on the Organisation to ensure that it had a sufficient understanding and appreciation of the product before making use of it, particularly where it will be used to collect, use and/or disclose personal data.

18 This is a position that was taken in *Re GMM Technoworld Pte. Ltd.* [2016] SGPDPC 18 ("***GMM Technoworld***"). In that case, the Organisation created an online warranty registration form using a third party paid plug-in for Wordpress which allowed for the capture of personal data on the website. However, as a result of the Organisation's misunderstanding and incorrect use of the functions of the Plug-in, the personal data of approximately 190 of its customers were displayed on its website.

---

2 See <https://gsuite.google.com/learning-center/products/forms/get-started/#!/>.

19 As observed in *GMM Technoworld* (at [12]):

> …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.
>
> [Emphasis added.]

20 In light of the absence of any security arrangements to protect personal data from such unauthorised disclosure, the Commissioner finds that the Organisation has contravened section 24 of the PDPA.

Directions

21 Having found the Organisation to be in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

22 In assessing the breach and determining the directions to be imposed, the Commissioner noted that the Appeal Form Data disclosed included the appeal statements which contained information about an individual driver's

suspension from the GrabHitch service. The Organisation has indicated that these suspensions were on the basis that the drivers were "gaming the system". In the Organisation's own view, such "gaming of the system", suggested a lack of probity on the part of the drivers. Such allegations could potentially cause actual or potential harm, injury or hardship, including reputational damage where disclosed without authorisation. Also, the personal data disclosed included Hitch Drivers' NRIC numbers. The aforesaid was treated as an aggravating factor.

23 The Commissioner also took into account the following mitigating factors:

(a) the personal data was only disclosed to a limited number of individuals;

(b) the Organisation took prompt action to mitigate the impact of the breach by removing access to the Google Form within the same day that the Google Form was made available to the drivers. As such, the personal data was only disclosed for around 7 hours;

(c) the Organisation had cooperated fully with the investigation; and

(d) the Organisation had notified the Commission of the Incident, albeit after the Commission had received a complaint from one of the affected Hitch Drivers.

24 The Commissioner has also considered the representations made by the Organisation through their letter of 14 May 2018. The Organisation's representations were as follows:

(a) to reconsider the position that the Organisation did not have the relevant data protection policies in place. In this regard, when the Organisation was asked for copies of its policies and internal guidelines for the protection of personal data which were valid as at the time of the Incident, the Organisation replied that it was in the process of drafting the relevant standard operating procedures ("SOPs"). In its representations, the Organisation clarified that it did in fact have relevant data protection policies in place and that the reference to the SOPs was in fact an updated version of its data protection policies. The Commissioner has considered the evidence provided and accepts that the Organisation did in fact have in place a data protection policy at the time of the Incident;

(b) The Hitch Drivers' appeal cases did not involve allegations of safety or security offences and instead involved exceeding the allowed 2 trips per day or "gaming" the system and that this type of case was much less sensitive than the facts in *Re Credit Counselling Singapore* [2017] SGPDPC 18. The Commissioner had already taken this point into consideration in determining the quantum of the financial penalty.

25 The Commissioner, after reviewing the Organisation's representations as a whole, agreed to the Organisation's request for a reduction in the financial penalty initially proposed.

26 Having considered all the relevant factors of this case and the representations made by the Organisation as summarised above, the Commissioner hereby issues a direction to the Organisation to pay a financial penalty of $6,000.

YEONG ZEE KIN
DEPUTY COMMISSIONER
[FOR COMMISSIONER] FOR PERSONAL DATA PROTECTION