COMMISSIONER FOR PERSONAL DATA PROTECTION

[2019] SGPDPC 15

Case No DP-1801-B1526

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

And

(1) GrabCar Pte. Ltd. (UEN No. 201427085E)

… *Organisation*

DECISION

GrabCar Pte. Ltd.

Tan Kiat How, Commissioner — Case No DP-1801-B1526

11 June 2019

1 This case concerns the unauthorised disclosure of the names and mobile phone numbers of 120,747 GrabCar Pte. Ltd. (the "**Organisation**") customers in marketing emails sent out by the Organisation (the "**Incident**"). On 5 January 2018, GrabTaxi Holdings Pte. Ltd., a related corporation of the Organisation,[1] notified the Personal Data Protection Commission of the Incident on behalf of the Organisation. The Commissioner's findings and grounds of decision based on the investigations carried out in this matter are set out below.

Material Facts

2 The Organisation is part of the Grab Group, which offers, among other things, ride-hailing transport services, food delivery and payment services on its mobile platform. As part of its marketing strategy, the Organisation regularly conducts marketing campaigns to reach out to targeted customers. These frequently involves sending emails offering special promotions to selected customers.

3 On 17 December 2017, the Organisation sent out 399,751 marketing emails to a targeted group of customers as part of a marketing campaign ("**Marketing Campaign**"). Out of the emails sent on that date, 120,747 emails contained the name and mobile phone number[2] of another customer, i.e. the email was sent to User A's (the intended recipient) email address but User B's (the mismatched customer) name and mobile phone number was reflected in the email as that of the intended recipient (the "**Mismatched Emails**").

4 Shortly after the Mismatched Emails were sent out, the Organisation's Customer Experience team reported an increased number of customer queries regarding the unauthorised disclosure of their personal data to other customers. The Organisation commenced investigations immediately thereafter. It determined that the Incident was caused by the

[1] The Legal and Compliance team for the Grab Group in Singapore sits within GrabTaxi Holdings Pte. Ltd.

[2] A customer's mobile phone number is linked to their account and a customer's email address could be linked to several mobile phone numbers. As such, the customer's mobile phone number was included in the marketing emails to allow users to easily identify which of their accounts would be applicable for the promotion.

erroneous assembly of customer information from different database tables that could, in turn, be traced to changes that had been made to the structure of its customer database since the previous marketing campaign.

5 The Organisation maintains a set of user attributes, i.e. data points that describe every customer such as registration date, bookings and rides, in a database table (the "**Main Table**"). Each customer is assigned a unique "passengers_id" number in the Main Table. For the purpose of illustration, the Main Table would have appeared as follows:

passengers_id	**name**	**passenger_email**	**passenger_mobile_no**
12354567	Sally Goh	sal.g@amail.com	81456789
22558866	John Tan	jt@amail.com	84567894
76543211	Alex Lee	al@amail.com	91111212

6 On 24 November 2017, as part of the Organisation's email verification efforts,[3] the Organisation's Product Analytics team was instructed to add a new user attribute "is_email_verified". The verified email addresses were placed in a database table (the "**Verified Email Database Table**") which was separate from the Main Table. Each customer in the Verified Email Database Table was assigned a unique "verified_email_user_id" number. For the purpose of illustration, the Verified Email Database Table would have appeared as follows:

verified_email_user_id	**Name**	**verified_email**
22558866	Luke Kang	Luke.k@amail.com
76543211	Mindy Ho	Mindy.ho@amail.com
12354567	M. Hafiz	Hafizm@amail.com

In the above example, only Luke Kang, Mindy Ho and M. Hafiz had verified their emails and would be included in the Verified Email Database Table. Those customers who did not verify their emails would not be included in the Verified Email Database Table.

[3] The email verification exercise was undertaken to allow the Organisation to target customers with verified email addresses for future marketing campaigns.

7 The "passengers_ids" and "verified_email_user_ids" were created separately but both ID numbers are of the same integer length and comprise entirely of numerals (i.e. without alphabets or other symbols). Unbeknownst to the Organisation at the time, some "verified_email_user_ids" were identical to some "passengers_ids" even though they did not identify the same customer.

8 At the time of the Incident, the procedure for using new user attributes to generate and send marketing emails was as follows:

(a) Regional Marketing provides high-level marketing requirements;

(b) Product Analytics creates the corresponding database queries (which were SQL commands), that identify and select the attributes to be used in the marketing campaign. This process is subject to some internal tests;

(c) Data Engineering executes the database query to produce the data for the marketing campaign. The data file is then uploaded to an emailing system to generate the actual marketing emails for use in the campaign.

(d) Regional Marketing "verifies" the final outcome by looking at the marketing emails that have already been sent out, typically by including some test account email addresses in the email blast.

9 In the present case, Product Analytics, who wrote the SQL command for the database query for the Marketing Campaign, wrongly equated "verified_email_user_id" with "passengers_id" and treated them as the unique identifier for a customer. As a result of this error, the SQL command used "verified_email_user_ids" to select the attributes for producing the data to generate the campaign emails.

10 As a result, when the Data Engineering team used the SQL command to produce the data to generate marketing emails for the campaign, email addresses were drawn from the Verified Email Database Table whereas the customer's name and mobile phone number were drawn from the Main Table on the assumption that the "verified_email_user_id" and "passengers_id" referred to the same customer. The Mismatched Emails were therefore created where the "verified_email_user_id" in the Verified Email Database Table coincided with

another customer's "passengers_id" in the Main Table. Using the sample information from the tables at paragraphs 5 and 6 above, the consolidated table would have appeared as follows:

passengers_id	**name**	**passenger_mobile_no**	**verified_email_user_id**	**verified_email**
12354567	Sally Goh	81456789	12354567	Hafizm@amail.com
22558866	John Tan	84567894	22558866	Luke.k@amail.com
76543211	Alex Lee	91111212	76543211	Mindy.ho@amail.com

11 Using the above example, M. Hafiz (who had verified his email address) would have received an email at his verified email address, Hafizm@amail.com, with Sally Goh's name and mobile phone number because the SQL command for the database query equated "verified_email_user_id" with "passengers_id" and his "verified_email_user_id" is identical to Sally Goh's "passengers_id". Similarly, Luke Kang (who had verified his email address) would have received an email at his verified email address, Luke.k@amail.com, with John Tan's name and mobile phone number as his "verified_email_user_id" is identical to John Tan's "passengers_id". Mindy Ho would have received an email at her verified email address, Mindy.ho@amail.com, with Alex Lee's name and mobile phone number as her "verified_email_user_id" was identical to Alex Lee's "passengers_id".

12 Although a total of 399,751 marketing emails were generated and sent in the Marketing Campaign, only customers who had verified their email addresses[4] received the Mismatched Emails as they were the only ones that were assigned a "verified_email_user_id". Emails were not sent to those who did not verify their email address.

13 Following the Incident, the Organisation took the following remedial actions:

(a) the Organisation implemented more rigorous data validation and checks to the addition/changing of user attributes process;

(b) the Organisation changed its practices to require a third person to perform sanity checks of the data before triggering any new campaigns; and

[4] The 120,747 affected individuals.

(c) the Organisation plans to incorporate privacy by design elements by masking mobile phone numbers (eg. 9*****11) in future marketing campaigns.

Findings and Basis for Determination

14 The key issue for determination is whether the Organisation had complied with its obligations under section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

15 As a preliminary point, customer names and mobile phone numbers are personal data as defined under section 2(1) of the PDPA as it is clearly possible to identify the individuals from that data. It was also not disputed that the personal data was disclosed mistakenly and without authorisation.

Whether the Organisation complied with its obligations under section 24 of the PDPA

16 Section 24 of the PDPA requires an organisation to protect the personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

17 The Commissioner finds that the Organisation did not have adequate measures in place to detect whether the changes it made to the system that held personal data introduced errors that put the personal data it was processing at risk. As highlighted in *Re Flight Raja Travels Singapore Pte. Ltd.* [2018] SGPDPC 16 (at [8]):

> "… when an organisation makes changes to a system that processes personal data in its possession or control, *the organisation has to make reasonable arrangements to prevent any compromise to personal data.*"
>
> [Emphasis added.]

18 First, it is not disputed that the root cause of the Incident was an error with the database query command which erroneously treated the "verified_email_user_id" as the unique identifier when it joined data from two database tables. Essentially, the Organisation consolidated the Verified Email Database and the Main Table by equating the "verified_email_user_id" found in the Verified Email Database Table with the "passengers_id" found in the Main Table and running the command to extract the verified email address of its

clients from the Verified Email Database and the name and contact number of its clients from the Main Table. The result was that, where the "passengers_id" and the "verified_email_user_id" were coincidentally the same number, the command would have extracted the email address corresponding to the "verified_email_user_id" of a client from the Verified Email Database and matched it with the name and mobile number corresponding to the "passengers_id" of a different client from the Main Table. Therefore, the 1st client would have been sent an email from the Organisation with the name and mobile number of the 2nd client.

19 Second, the Commissioner finds that the Incident arose in part because of administrative failures. In this regard, the Organisation itself admitted that the technical documentation for the new Verified Email Database Table was not sufficiently clear. If the documentation had been clearer, the employee who wrote the SQL command for the database query might not have made the erroneous assumption and would not have joined the two database tables in that way.

20 Finally, there were shortcomings in the way the Organisation conducted tests. Tests were conducted on non-verified email addresses instead of on both non-verified and verified email addresses. The core team of testers did not discover the mismatch between the customer's email address and his/her name and mobile number because the test email addresses used were not verified email addresses and were therefore not affected by the erroneous joining.

21 There was another grave error in this case. Investigations disclosed that there had not been proper user acceptance testing of the SQL script before it was deployed into production. Product Analytics conducted technical tests but Regional Marketing was not involved in user acceptance testing. The Regional Marketing team only verified the actual production run of emails, i.e. emails that were already sent to customers. Hence, even if they detected any errors such as the mismatched data, it would have been too late to correct the error.

22 In the circumstances, the Commissioner finds that the Organisation had failed to make reasonable security arrangements to detect errors when preparing the change, i.e. writing the database query, as well as in failing to conduct proper testing before implementing the change. It is therefore in breach of section 24 of the PDPA.

Directions

23 Having found that the Organisation is in breach of the Protection Obligation under 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.

24 In assessing the breach and determining the directions to be imposed, the Commissioner took into account the following mitigating factors:

(a) the Organisation was cooperative during the investigation and in line with their implementation of their data breach management plan they notified the Commission voluntarily;

(b) the Organisation took immediate effective remedial action in line with their implementation of their data breach management plan;

(c) the personal data disclosed compromised only the individual's name and mobile phone number, which was not of a sensitive nature; and

(d) the affected customer's personal data was only disclosed to one individual, i.e. a customer whose "passengers_id" was identical to the affected customer's "verified_email_user_id" number.

25 The Organisation made representations to the Commission after the preliminary grounds of decision was issued and requested for a reduction in the financial penalty of $16,000 provided in the said preliminary grounds of decision. The Organisation based this request on their prompt voluntary notification and implementation of a remediation plan, and the financial penalty amounts imposed in previous cases. In particular, the Organisation cited the cases of Re Aviva Ltd [2017] SGPDPC 14, Re NTUC Income Co-operative Ltd [2018] SGPDPC 10, Re Flight Raja Travels Singapore [2018] SGPDPC 16 and Re Challenger Technologies and another [2016] SGPDPC 6.

26 The Organisation's voluntary notification and accountable practices had already been taken into account in assessing the financial penalty.

27 The cited cases are distinguishable from the present case. In *Re Aviva Ltd* and *Re NTUC Income Co-operative Ltd*, the financial penalty imposed was $6,000 and $10,000 respectively. The reason that this case warrants a higher financial penalty even though it does not involve sensitive personal data (unlike in the previous two cases), is the much higher number of individuals affected. In this case, a total of 120,747 data subjects were affected, while only 2 data subjects were affected in *Re Aviva Ltd* and 214 data subjects were impacted in *Re NTUC Income Co-operative Ltd*. Similarly, only 72 data subjects were impacted in *Re Flight Raja Travels Singapore*.

28 *Re Challenger Technologies* and *another* was one of the first grounds of decisions which were issued. The Commission had taken into consideration the fact that the incident in that case happened in September 2014, only a few months after the coming into force of the PDPA, when organisations may not have understood fully the manner in which they were required to comply with their obligations. After more than 4 years since the PDPA has come into full force, this consideration is no longer applicable and organisations should not be referring to these early cases in estimating the quantum of the potential financial penalties that may be imposed.

29 The Commissioner hereby directs the Organisation to pay a financial penalty of S$16,000 in accordance with 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 such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION