23 September 2020

CASE NOTE – DATA PROTECTION

Breach of Protection Obligation

Grabcar Pte Ltd [2020] SGPDPC 14

On 21 July 2020, the Personal Data Protection Commission ("**PDPC**") ordered Grabcar Pte Ltd ("**Grabcar**") to pay a financial penalty of S$10,000. This is the fourth time that Grabcar has been found in breach of its protection obligation under the Personal Data Protection Act ("**PDPA**"), a fact that did not escape the PDPC's notice. In light of the repeated infractions by Grabcar of its data protection obligations, the PDPC also directed Grabcar to put in place a data-protection-by-design policy for its mobile applications, in a bid to reduce the risk of further data breaches.

Background

Grabcar is a Singapore-based company offering ride-hailing transport services, food delivery and digital payment solutions through its mobile application (the "**Grab App**"). One of the features offered in the Grab App is a carpooling option referred to as "GrabHitch", which matches a passenger with a driver willing to give a lift to the passenger in return for a fee.

This case centred on a recent update rolled out by Grabcar to address a potential vulnerability in the Grab App. Ironically, the update resulted in a total of 21,541 GrabHitch drivers' and passengers' data being exposed to the risk of unauthorised access.

The vulnerability sought to be addressed by Grabcar was that the application programming interface endpoint ("**URL**") that allowed GrabHitch drivers to access their own data contained a "userID" portion that could potentially be manipulated to allow access to other GrabHitch drivers' data.
In its update, Grabcar removed the variable 'userID' from the URL. However, it failed to take into account the URL-based caching mechanism in the Grab App which was configured to refresh every 10 seconds. This caching mechanism served cached content in response to data requests to reduce the load of direct access to the Grabcar's database.

Without the variable 'userID' in the URL (which directed data requests to the correct GrabHitch driver's account), the caching 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 Grabcar database and cached for the next 10 seconds.

As a result, personal data belonging to GrabHitch drivers and passengers were exposed to risk of unauthorised access, including profile pictures, passenger names; vehicle plate numbers, and wallet balances comprising journal history of ride payments.

Upon being notified of the incident, Grabcar took a number of remedial measures, including rolling back the app to the version prior to the update within 40 minutes, and notifying a number of the affected GrabHitch drivers of the incident the same day.

PDPC's decision

Unsurprisingly, the PDPC held that Grabcar failed to put in place reasonable security arrangements to prevent any compromise to personal data in its possession and under its control, as Grabcar failed to put in place sufficiently robust processes to manage changes to its IT system. Specifically, Grabcar introduced changes to the Grab App without understanding how the changes would operate with existing features of the Grab App and its broader IT system, including the caching mechanism.

What was notable was that the PDPC found Grabcar's failure a particularly grave error, as this was the second time Grabcar was making a similar mistake, albeit with respect to a different system. In the earlier decision *Re Grabcar Pte Ltd* [2019] SGPDPC 15 in June 2019, the PDPC determined that Grabcar had made changes to its marketing system and database (containing personal data) without adequate measures in place to detect whether such changes introduced errors that put the personal data it was processing at risk. As a result, Grabcar inadvertently disclosed the names and mobile phone numbers of 120,747 customers in marketing e-mails without authorisation, and was fined S$16,000.

It should also be highlighted that in both instances, Grabcar did not conduct properly scoped testing before the respective updates to its IT systems were deployed. Such tests prior to deployment are critical to detect and rectify errors in new IT features and/or be alerted to any unintended effects from changes that may put personal data at risk.

Given that this was the fourth time that Grabcar was found in breach of its protection obligation, and further that Grabcar's business involves processing large volumes of personal data on a daily basis, the PDPC found this to be a significant cause for concern, and took this into account when meting out a penalty to Grabcar.

Key Takeaways

Merely putting in place policies and procedures to prevent security breaches is insufficient. Instead, each organisation should aim to have a holistic understanding of its existing IT infrastructure, along with its risks and vulnerabilities – particularly when making changes to its systems. At the minimum, tests should be run that reflect an understanding of the organisation's normal operating environment. The PDPC has indicated that a lack of such properly scoped tests would not meet the requirement for reasonable security arrangements. The meeting of data security standards should be included in test criteria for systems which process personal data, to ensure that no personal data may be accessed or disclosed during operational use. It is also worth noting that the PDPC also scrutinises the nature of any repeat offences, and will come down more harshly on organisations that repeatedly commit similar mistakes, even across differing systems.

For queries or more information, please contact:

Wilson Wong
Director
wilson.wong@amicalaw.com
(65) 6303 6213

Anna Toh
Associate Director
anna.toh@amicalaw.com
(65) 6303 6234

Geraldine Tan
Director
geraldine.tan@amicalaw.com
(65) 6303 6231

Dawn Chua
Legal Associate
dawn.chua@amicalaw.com
(65) 6303 8191