



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**IN RE: GRAB PHILIPPINES' [1]
ROLL-OUT OF THE PASSENGER
SELFIE VERIFICATION; [2] PILOT
TEST OF THE IN-VEHICLE AUDIO
RECORDING; AND [3] PILOT TEST
OF THE IN-VEHICLE VIDEO
RECORDING**

NPC CC 20-001

x-----x

CEASE AND DESIST ORDER

NAGA, D.P.C.:

This resolves the Recommendation of this Commission's Data Security and Compliance Office ("DASCO") to issue a Cease and Desist Order¹ directing Grab Philippines ("Grab PH") to suspend the pilot test and any plans to roll out their three (3) new data processing systems, namely: Passenger Selfie Verification, In-Vehicle Audio Recording, and In-Vehicle Video Recording (collectively referred to as "three (3) new data processing systems") due to the discovered deficiencies that may endanger the privacy rights of the riding public.

FACTS

On 15 January 2020, a conference was held between the Commission and Grab PH to discuss the features, data privacy measures, and other details of its three (3) new data processing systems. During the said meeting, Grab submitted the following documents: Privacy Impact Assessment of the three (3) new data processing systems, Personal Data Review, Grab PH Data Protection Handbook, and Powerpoint presentation on the three (3) new data processing systems.

Based on the submitted documents of Grab PH and their statements during the conference, the features of the three (3) new data processing systems can be described in this wise:

¹ Dated 31 January 2020

1. Passenger Selfie Verification is a process of identity verification adopted by Grab PH wherein passengers are prompted through the Grab application to follow the on-screen instructions, ultimately requiring them to take a selfie. This is one of the modes by which Grab verifies the identity of its passenger.

According to Grab PH, the selfie generated will be used solely for verification and will not be shared with the driver. However, the data can also be provided as evidence in the event of disputes, conflicts, and or complaints.

During the meeting, Grab PH said that the retention period of the selfies is seven (7) years.

2. The In-vehicle Audio Recording is the process by which conversations transpiring inside the vehicle during the trip are being documented by audio-recording via the driver's Grab application. It is currently implemented as a pilot test that will run for two (2) weeks among ninety (90) Grab PH drivers.

The recording starts from the moment the passenger is picked up until drop off at the pinned destination. According to Grab PH, the audio recording is encrypted with AES 256 bits key and asymmetric encryption with a seven (7) day retention period.

3. The In-vehicle Video Recording is the process through which Grab PH documents the passenger and driver experience during the trip with the use of an in-vehicle video camera powered by the electrical system of the vehicle.

It is currently implemented as a pilot test that will run for six (6) weeks among ninety (90) Grab PH drivers.

For the In-Vehicle Audio and In-Vehicle Video Recording, Grab PH said that these systems are being piloted to promote the safety of both the drivers and passengers.

After reviewing all the submitted documents of Grab PH and the representations they made during the 15 January 2020 conference,

DASCO issued a Notice of Deficiencies to Grab PH in relation to its three (3) new data processing systems, to wit:

1. In June 2019, it was estimated that **one of six Filipinos has installed a Grab app**, all of whom could be potentially affected by risks arising from the aforementioned processing. Despite the possible impact, **Grab did not sufficiently identify and assess the risks posed by its data processing systems to the rights and freedoms of data subjects**. Its PIA methodology states that “The impact to Grab when a risk becomes reality is assessed under the four major categories of operational downtime, people, reputational damage and financial loss”, clearly indicating that only the risks faced by the company were taken into account. The sole risk that Grab PH included in its PIA was “regulation action being taken for lack of consent and notification to individuals”. **(Emphasis supplied)**

As a result, the controls identified only corresponded to the said risk. **The PIA did not include controls to secure the photo, audio and video recording from unauthorized disclosure or access, accidental or unlawful destruction, loss, and alteration**. These should have been considered in the PIA given the sensitivity of the data, the use of third party providers, and the fact that Grab collects several other personal data through other systems (e.g. user profile creation/registration, linking Grab account to social media accounts, GrabPay, etc.). Both factors make Grab and its systems a very attractive target of hacking attacks. **(Emphasis supplied)**

2. During the meeting, Grab explained that the photo, audio and video files will be provided to authorities if they get a verified police request after an incident. **According to Grab, the audio and video files will be used as evidence in the event of dispute, conflict, or complaint**. The video recording system will also enable Grab employees to monitor the situation live from the Grab Office and take photos of what is happening inside the vehicle, once the driver prompts the office through the emergency button. **(Emphasis supplied)**

However, none of these were reflected in its privacy notice (Grabchat message and email) and policy. Affected data subjects only received Grabchat messages and emails that stated a generic purpose—that the processing was “for safety and security purposes”, “to improve passenger and driver safety”, and “to make riding safer”. A link to the second layer information was included in the Grabchat messages, which was supposed to provide the complete and specific details about the processing. The link, however, leads the passenger to Grab’s Privacy Policy which only provides a high-level view of all the processing systems of Grab. **(Emphasis supplied)**

3. **Grab did not communicate the basis it uses for the processing to be considered lawful**. It should have indicated if the processing was

pursuant to a regulatory requirement of another authority or if it is **based on the legitimate interests** of the company and its customers. If the processing was based on the latter, Grab could have cited documented in-vehicle incidents and other related information in the PIA, which may serve as evidence for the existence of a legitimate interest. **(Emphasis supplied)**

4. The **submitted documents were not able to show if the processing was proportional to its purpose**. The PIA lacked the information on whether the benefits of the processing systems were found to outweigh the risks. It had no information if Grab assessed that the passenger selfie verification and the in-vehicle audio and video recording were indeed the best alternatives among all identified means to achieve the underlying purpose. Likewise, it was unclear if Grab assessed whether the personal data it collects from these processing systems are not excessive. **(Emphasis supplied)**
5. **Having the option to withdraw consent was one of the controls included in the PIA for the pilot test of the in-vehicle audio and video recording. However, the mechanism to exercise such right during and after the ride was not spelled out in the Grabchat message**. It was also not specified if and how the processing will stop if the passenger withdraws consent during the ride, considering that the tech specs prevent the driver from having any control over the device. Further, it was unclear how the consent mechanism will work if Grab decides to roll out the system which may necessitate that all Grab cars be equipped with the recording device. **(Emphasis supplied)**

During the conference, Grab said that they can provide passengers a copy of the audio and video recording when requested. But the Grabchat message was not explicit about this, nor was it clear on how passengers can actually exercise this and other data privacy rights. It also lacked the contact details of the Data Protection Officer of Grab PH. The purpose of the processing may be partly defeated if these information are not provided to the riding public.

6. **The PIA and the notice/email for the passenger selfie verification were silent about the storage and retention period of the photos**. As to the pilot test, Grab stated that the “video recordings will be stored with the provider”, and “the encrypted audio is temporarily stored on Grab servers” in its PIA and Grabchat message, respectively. It did not specify, however, whether these servers are located in or outside the country, which should be a consideration when determining the appropriate security measures to implement. Should the servers be located outside the country, Grab simply assumes that the data subject allows such cross-border data transfer since its Privacy Policy states that, “You understand and consent to the transfer of your personal data from your Home Country to the Alternate Country”. Under the law, data subjects must be made aware of these information. **(Emphasis supplied)**

Given these deficiencies, Grab PH must adopt the appropriate measures to correct or remedy the same. As such, Grab PH is hereby **DIRECTED** to comply with the following:

1. Conduct/update the PIA for the processing systems according to NPC Advisory 2017-03, using a methodology that meets the following criteria:
 - a. Provides a systematic description of the personal data flow and processing activities including the purpose of the processing, data inventory identifying the types of personal data held, sources and procedures of collection, functional description of the processing including information repositories, data transfers, storage and disposal method of personal data, accountable and responsible persons involved in the processing, and existing organizational, physical and technical security measures;
 - b. Includes an assessment of Grab's adherence to the data privacy principles, implementation of security measures, and the provision of mechanisms for the exercise of data subject rights;
 - c. Identifies and evaluates the risks posed by the processing, and proposes measures to address the risks; and
 - d. An inclusive process that ensures the involvement of interested parties and secures inputs from the DPO and data subjects; and
2. Based on the updated PIAs, update the Privacy Notices and Privacy Manual / Data Protection Handbook.

On a Memorandum dated 31 January 2020, the DASCO recommended to this Commission the issuance of Cease and Desist Order for Grab PH to suspend the [1] roll-out of the Passenger Selfie Verification; [2] pilot test of the In-Vehicle Audio Recording; and [3] pilot test of the In-Vehicle Video Recording until such time that Grab PH fully implements the proper controls to address the deficiencies identified in the Notice of Deficiencies. Further, DASCO emphasized that the issuance of the Cease and Desist Order is in pursuit of protecting public interest by mitigating the risks posed by these processing systems to data subjects.

DISCUSSION

The power of this Commission to issue Cease and Desist Order is explicitly provided in Section 7(c) of the Data Privacy Act (“DPA”), thus:

“Section 7(c). Issue **cease and desist orders**, impose a temporary or permanent ban on the processing of personal information, **upon finding that the processing will be detrimental to national security and public interest.**” (Emphasis supplied)

The same power was reiterated in Section 9.f.3 of the Implementing Rules and Regulations of the DPA, to wit:

“Section 9. *Functions*. The National Privacy Commission shall have the following functions:

xxxxx xxxxx xxxxx

f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:

xxxxx xxxxx xxxxx

3. Issuing **cease and desist orders**, or imposing a temporary or permanent ban on the processing of personal data, **upon finding that the processing will be detrimental to national security or public interest**, or if it is necessary to **preserve and protect the rights of data subjects**.” (Emphasis supplied)

From the plain reading of the DPA and its IRR, there are only two (2) elements needed in order for this Commission to validly exercise its power to issue Cease and Desist Order, to wit:

1. There must be a finding or determination; and
2. The processing of personal data will be detrimental to **national security, public interest**, or the **issuance is necessary to preserve and protect the rights of the data subject**.

In DASCO Notice of Deficiencies dated 31 January 2020, it was clearly established that Grab PH's three (3) new data processing systems' risk assessment and mitigation are lacking, the PIA and privacy notice are insufficient, and the purpose of data processing itself is unclear. Further, in DASCO Memorandum dated 31 January 2020, it was stated that, "maintaining the status quo, wherein Grab PH is engaged in the collection and processing of passenger personal information through the processing systems in question, would further expose the fundamental rights and freedoms of the concerned data subjects to detrimental risks."

While this Commission believes that the security of passengers and drivers is a primordial concern, their privacy rights must not be disregarded. It must be protected with earnestness by ensuring that the purpose of data processing is clearly stated, the data flow is secured, and the risks are properly identified and mitigated. Absent these safeguards, this Commission will always adhere in protecting the privacy rights of the data subjects.

WHEREFORE, premises considered, Grab PH is hereby ordered to **CEASE AND DESIST** the [1] roll-out of the Passenger Selfie Verification; [2] pilot test of the In-Vehicle Audio Recording; and [3] pilot test of the In-Vehicle Video Recording until such time that Grab PH fully satisfies the requirements of this Commission as stated in the 31 January 2020 Notice of Deficiencies issued by DASCO.

SO ORDERED.

Pasay City, Philippines
03 February 2020

[SGD.] JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

[SGD.] RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[SGD.] LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner