Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2020-054[1]

28 December 2020

[redacted]

Re: PERSONAL DATA COLLECTION AND RETENTION USING QR CODES FOR CONTACT TRACING

Dear [redacted]

We write in response to your query seeking guidance on an issue involving the proposed implementation by the local government of Iloilo City of a COVID-19 contract tracing system using a unique and permanent Quick Response (QR) Code.

Under this system, individuals who are residents of, non-residents who work in, and non-residents who wish to visit Iloilo City shall be required to register and secure their respective unique and permanent QR Codes. Both private and government offices, including private business establishments, within Iloilo City shall adopt a "NO QR CODE, NO ENTRY" policy for their respective offices as implementation of said contract tracing system.

As mentioned in your letter, personal information in relation to the contract tracing system shall be gathered, recorded, and accessed solely by the city government and will be used to detect and identify possible close contacts of confirmed COVID-19 case/s.

Specifically, you ask for guidance on the following:

(1) Whether the age and date of birth of data subjects may be required for registration and to secure their respective QR Codes; and

(2) Whether the data collected in relation to the contact tracing system may be stored for a longer period, or at the very least until the COVID-19 pandemic has ended.

[1] Tags: criteria for processing sensitive personal information; proportionality; retention; disposal; contact tracing

Processing of sensitive personal information; lawful criteria; law or regulation; COVID-19 surveillance; proportionality

Under the Data Privacy Act (DPA) of 2012,[2] information about an individual's age as well as date of birth, which is a variation of age, are considered as sensitive personal information (SPI). The processing for SPI finds basis under any of the lawful criteria for processing under Section 13 of the DPA, one of which is the processing that is provided for by existing laws and regulations.[3]

We relate the above to the collection of age and date of birth of data subjects pursuant to the relevant Department of Health (DOH) issuances: Department Memorandum (DM) No. 2020-0189 (Updated Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases), DM No. 0436 (Minimum Data Requirements of COVID-19-Related Information Systems), and Department Circular No. 2020-0318 (Mandatory Submission of Accurate, Complete, and Timely COVID-19 Case Data through the COVID Document Repository System (CDRS) and Laboratory Information System API). All these issuances discuss the use of the COVID-19 Case Investigation Forms (CIF).

We understand that the accomplishment of the CIF happens only for data subjects or the type of client, as referred to in the form, who are any of the following:

- COVID-19 Case (Suspect, Probable, or Confirmed);
- For RT-PCR Testing (Not a Case of Close Contact); or
- Close Contact.

We understand also that the CIF is meant to be administered as an interview by a health care worker or any personnel of the Disease Reporting Units (DRU) concerned.

Hence, the collection of data in the scenario above is clearly distinct from the collection of data by the city government at the very initial stages, i.e. for the identification of possible close contacts of confirmed COVID-19 case/s through the QR Codes. These data subjects are not yet suspect, probable, or confirmed cases nor close contacts. These persons are just employees, clients, and/or visitors or simply just passing through private and government offices or business establishments at that point in time when they happen to enter a particular location.

On the other hand, while the city government may have the prerogative to require such personal data through an executive order, ordinance, or some other issuance or regulation, it is best that a judicious assessment should first be made on whether the age and date of birth of data subjects, as well as any other personal data proposed to be collected, are necessary and indispensable to the implementation of the subject contact tracing system.

The Supreme Court held in Dela Cruz vs. Paras[4] that "ordinances passed by virtue of the implied power found in the general welfare clause must be reasonable, consonant with the general powers and purposes of the corporation, and not inconsistent with the laws or policy of the State."

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 13 (b).
[4] Dela Cruz vs. Paras, 208 PHIL 490 (1983).

We must be reminded that any city government issuance that would govern the implementation of the subject contact tracing system must be in consonance with other issuances for the COVID-19 response. Specifically pertinent in this scenario is the issuance of the Department of Trade and Industry (DTI) and the Department of Labor and Employment (DOLE) on the Workplace Prevention and Control of COVID-19. Please refer to the same for additional guidance on the matter.

Note that the proportionality principle should be duly considered. This principle dictates that the processing of personal data should be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[5]

Retention period; disposal of collected sensitive personal information

Personal data must be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained.[6]

We refer to the provisions of NPC Advisory No. 2020 – 03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response, specifically its provisions on storage and retention:

> "6. All personal data collected for the purpose of contact tracing shall be retained only for the period allowed by existing government issuances. The DTI-DOLE JMC provides that personal data collected through the health declaration form or the visitor contact tracing form shall be stored only for a limited period and shall be disposed of properly after thirty (30) days from date of accomplishment.
>
> 7. All other personal data collected for the management of probable, suspected and confirmed COVID-19 patients shall be stored only for as long as necessary or when the purpose for processing still exists."[7]

Thus, there is a need to distinguish those personal data or records to be stored in the QR code: those which may be retained for as long as there is a state of public health emergency necessitating the need for such system, i.e. name and other contact details, and those which should be routinely disposed of, i.e. records of the locations where the QR code was scanned, etc., which may be similar to the health declaration form or the visitor contact tracing form in the DTI-DOLE issuance, the retention of which is only thirty (30) days.

Right to erasure

We emphasize that this right is not absolute. There are certain instances where the same may be exercised upon discovery and substantial proof of any of the following:

a. The personal data is:
    a. incomplete, outdated, false, or unlawfully obtained;
    b. being used for purpose not authorized by the data subject;

[5] *Id*. § 18 (c).
[6] Data Privacy Act of 2012, § 11 (e).
[7] National Privacy Commission, Guidelines for Workplaces and Establishments Processing Personal Data For Covid-19 Response [NPC Advisory No. 2020 – 03] (23 October 2020).

c. no longer necessary for the purposes for which they were collected; or

b. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
c. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
d. The processing is unlawful; or
e. The personal information controller or personal information processor violated the rights of the data subject.[8]

Note also that a request for erasure may be denied when personal data is still necessary for the fulfillment of the purpose/s for which the data was obtained and compliance with a legal obligation which requires personal data processing, among others.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[8] Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (e) (1).