Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular No. 2021-02

DATE : **08 November 2021**

SUBJECT : **GUIDELINES ON THE PROCESSING OF PERSONAL DATA DURING PUBLIC HEALTH EMERGENCIES FOR PUBLIC HEALTH MEASURES**

WHEREAS, the National Privacy Commission (NPC) supports the implementation of prevention, detection, isolation, treatment, and reintegration strategies of the national government agencies and local government units for the COVID-19 response, which includes contact tracing efforts and vaccine deployment;

WHEREAS, the NPC is cognizant of the vital role of data-driven technologies such as the development of contact tracing applications and vaccine card systems and applications which inevitably involve the processing of personal information;

WHEREAS, Section 11 of the Data Privacy Act of 2012 (DPA) allows for the processing of personal information, subject to the compliance with the requirements of the law and adherence to the general principles of transparency, legitimate purpose, and proportionality, among others;

WHEREAS, Sections 12 and 13 of the DPA enumerates the criteria for lawful processing of personal information, sensitive personal information, and privileged information (collectively, personal data);

WHEREAS, pursuant to Section 7 of the DPA, the NPC is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers with the provisions of the Act, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, Section 9 of the Implementing Rules and Regulations (IRR) of the DPA provides that, among the Commission's functions, is to develop, promulgate, review or amend rules and regulations for the effective implementation of the DPA;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the processing of personal data in the implementation of public health measures during public health emergencies.

SECTION 1. ***Scope.*** **—**The provisions of this Circular shall apply to all personal information controllers (PICs) and personal information processors (PIPs) engaged in the processing of

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

personal data during the COVID-19 public health emergency within the general framework of the necessary public health measures.

The relevant portions of the following sections of this Circular shall likewise apply to all future public health emergencies: Section 3 on General Principles, Section 4 on Criteria for lawful processing and purpose, Section 5 on Further processing and limitation, Section 7 on Privacy Impact Assessment, Section 8 on Privacy Notice, Section 9 on Application (app) permissions, Section 10 on Security Measures, Section 11 on Mandatory Submission of List of CTAs and Vaccine Card Systems, Section 12 on Storage and Retention, Section 13 on Disposal of personal data and decommissioning of CTAs and Vaccine Card Systems, and Section 14 on Data subject rights.

SECTION 2. ***Definition of Terms.*** **—** For the purpose of this Circular, the following terms are defined, as follows:

A. "Act" or "DPA" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

B. "Application Programming Interface" or "API" refers to a set of well-defined methods, functions, protocols, routines or commands which application software uses with facilities of programming languages to invoke services;[1]

C. "Commission" or "NPC" refers to the National Privacy Commission;

D. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.;

E. "Contact Tracing" refers to the identification, listing, and follow-up of persons who may have come into contact with a confirmed COVID-19 case. Contact tracing is an important component in containing outbreaks of infectious diseases. Under Code Red Sublevel 2, contact tracing is aimed at mitigating the spread of the disease;[2]

F. "Contact Tracing Application" or "CTA" refers to data processing systems[3] specifically designed to accomplish or support contact tracing;

G. "COVID-19 Vaccination Program" refers to the response of the national government in addressing the adverse impact of COVID-19 through the delivery and administration of both procured and donated COVID-19 vaccines, management of

[1] See: International Organization for Standardization, ISO/TS 23029:2020(en) Web-service-based application programming interface (WAPI) in financial services, *available at* https://www.iso.org/obp/ui/#iso:std:iso:ts:23029:ed-1:v1:en (last accessed June 19, 2021).
[2] Department of Health, Update Guidelines on Contact Tracing of Close Contacts of Confirmed Coronavirus Disease (COVID-19) Cases, Department Memorandum No. 2020-0189 (April 17, 2020).
[3] National Privacy Commission, Registration of Data Processing Systems and Notifications regarding Automated Decision-Making Operations [NPC Circular No. 17-01], § 3 (F): "Data Processing System" refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Adverse Event Following Immunization (AEFI) and indemnification as covered under the Republic Act No. 11525 or the or the COVID-19 Vaccination Program Act of 2021;[4]

H. "Data Protection Officer" or "DPO" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the DPA, its IRR, and other issuances of the Commission: *provided*, that a government agency or private entity may have more than one DPO;

I. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

J. "Decommissioning" refers to a process by which a business application (or system) is removed from use in an organization. It requires analysis of the data in the system, identifying the data, metadata and system documentation that must be brought forward and retained, and an accountable process for deletion of residual data in the system;[5]

K. "DOH Partner Agency" refers to the Department of Health (DOH) designated/deputized public health authority to collect and process COVID-19-related data for the purpose specified under the DOH and NPC Joint Memorandum Circular No. 2020-0002;[6]

L. "Government Agency" refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

M. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173;

N. "Personal data" refers to all types of personal information and sensitive personal information;

O. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

P. "Personal information controller" or "PIC" refers to a natural or juridical person, or any other body, who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

    1. A natural or juridical person, or any other body, who performs such functions as

[4] See: Department of Health and the National Task Force Against COVID-19, Rules and Regulations Implementing Republic Act No. 11525 [Joint Administrative Order No. 2021-0001], § V (E), (March 26, 2021).
[5] See: NSW State Archives, Decommissioning systems: records and information management considerations, *available at* https://www.records.nsw.gov.au/recordkeeping/advice/decommissioning-systems#:~:text=Decommissioning%20is%20a%20process%20by,from%20use%20in%20an%20organisation (last accessed June 19, 2021).
[6] Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002 (April 24, 2020).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is processed, or the purpose or extent of its processing.

Q. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data;

R. "Privacy by Design" is an approach that ensures that privacy and data protection have been taken into account during the design phase of a system, project, program and process and will continue to be taken into account throughout its lifecycle and implementation;

S. "Privacy enhancing technologies" or "PETs" also known as "Privacy-preserving methodologies" is a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the data system.[7] PETs ranges from tools that provide anonymity to those that allow a user to choose if, when, and under what circumstances personal information is disclosed.[8]

T. "Private entity" refers to any natural or juridical person, or any other body that is not a unit of the Philippine government or any other foreign government entities, such as but not limited to, stock and non-stock corporations, foreign corporations, partnerships, cooperatives, sole proprietorships, or any other legal entity;

U. "Privacy Impact Assessment" is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations;

V. "Privileged information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

W. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

[7] See: European Union Agency For Network And Information Security, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan, *available at* https://www.enisa.europa.eu/publications/pets (last accessed October 5, 2021).
[8] Ibid.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

X. "Public Health Authority" refers to the Department of Health (DOH), specifically the Epidemiology Bureau, Disease Prevention and Control Bureau, Bureau of Quarantine and International Health Surveillance, Health Emergency Management Bureau, Food and Drug Administration, government hospitals, Research Institute for Tropical Medicine and other National Reference Laboratories, and DOH Regional Offices, the local health office (provincial, city or municipality), or any person directly authorized to act on behalf of the DOH or the local health office;[9]

Y. "Public Health Emergency" refers to an occurrence or imminent threat of an illness or a health condition that poses a high probability of a large number of deaths in the affected population; a large number of serious injuries or long-term disabilities in the affected population; widespread exposure to an infectious or toxic agent that poses a significant risk of substantial harm to a large number of people in the affected population; and international exposure to an infectious or toxic agent that poses a significant risk to the health of citizens of other countries;[10]

Z. "Sensitive personal information" refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

AA. "System architecture" refers to a single, high-level, description of the major elements or objects of a system plus the inter-connections between them.[11]

BB. "Threat modeling" refers to a systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.[12]

SECTION 3. ***General principles.*** **—** The processing of personal data in response to public health emergencies as part of a public health measure, specifically the prevention, detection, isolation, treatment, and reintegration strategies such as but not limited to testing, contact

[9] An Act Providing Policies and Prescribing Procedures on Surveillance and Response to Notifiable Diseases, Epidemics, and Health Events of Public Health Concern, and Appropriating Funds Therefor, Repealing for the Purpose Act No. 3573, Otherwise Known as the "Law on Reporting of Communicable Diseases [Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act], Republic Act No. 11332, § 3 (k) (2019).
[10] Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act, § 3 (l).
[11] See: International Organization for Standardization, ISO/TR 26999:2012(en), Intelligent transport systems, § 2.15, *available at* https://www.iso.org/obp/ui/#iso:std:iso:tr:26999:ed-1:v1:en (last accessed October 19, 2021).
[12] See: International Organization for Standardization, ISO/IEC/IEEE 24765:2017(en), Systems and software engineering, § 3.4290, *available at* https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:en (last accessed October 19, 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

tracing, treatment, and activities relating to vaccine deployment, is recognized, and shall be governed by the following principles:

A. *Transparency.* PICs shall provide the necessary privacy notices at the appropriate instances in relation to all personal data processing activities for public health emergencies to adequately inform data subjects of the details of the processing of their personal data and their rights under the DPA;

B. *Legitimate purpose.* The specific purpose/s for personal data processing in response to public health emergencies as part of a public health measure shall be clearly determined prior to any personal data processing activities;

C. *Proportionality.* The processing of personal data shall be limited to the extent necessary to fulfill the identified legitimate purpose/s. Privacy enhancing technologies or privacy-preserving methodologies shall be employed to the end that personal data shall be processed only if the purpose of the processing could not be reasonably fulfilled by other means;

D. *Safeguards.* PICs shall implement appropriate measures, taking into account the integration of privacy by design and risk management in the development of systems and other digital tools where privacy is embedded into the design and architecture of the same and integral to the system without diminishing functionality;[13]

E. *Data subject rights.* PICs shall recognize and uphold the rights of affected data subjects, unless otherwise provided by law;[14] and

F. *Compliance and accountability.* PICs shall fulfill all applicable requirements prescribed by the DPA, its IRR, and other issuances of the NPC.

SECTION 4. ***Criteria for lawful processing; purpose.*** **—** A lawful basis for processing is necessary for all personal data processing activities as part of the response to public health emergencies:

A. Personal data processing shall be based on the applicable laws, rules, and regulations requiring the collection and use of personal data for a public health measure; and

B. Personal data collected as part of the response to public health emergencies shall not be repurposed for direct marketing, profiling, or any other analogous purpose, whether commercial or non-commercial.

[13] See generally: Cavoukian, Ann Ph.D., Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, *available at* https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (last accessed 21 Jan 2021) and 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, § 20 (2012).

[14] 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 § 16 (2012); Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34-37 (2016); and National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01] (January 29, 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

SECTION 5. ***Further processing; limitation.*** **—** Further processing of personal data may be allowed in instances which are compatible or consistent with the response to public health emergencies as part of public health measures, such as but not limited to historical, statistical, or scientific purposes.

A. The further processing is considered incompatible when:

    1. It would be very different from the original purpose of responding to public health emergencies as part of public health measures or there is no clear and reasonable link between such original purpose and the purposes of the intended further processing;
    2. It would result in an unjustified consequence on the rights and freedoms of the data subject;[15] or
    3. It would not be reasonably expected by the data subject considering the context in which the personal data has been collected.

    Further processing shall only be allowed when upon examination, it is determined to be compatible with the original purpose communicated to the data subject and not beyond what the data subject may reasonably expect as to the purpose, scope, manner, and extent of the processing of their personal data.[16]

B. The processing for research purposes may be allowed only when the same is intended for a public benefit and subject to the requirements of applicable laws, regulations, and ethical standards such as those prescribed by various research ethics boards or committees of the government, academic institutions, and other similar organizations prescribing such standards: *provided,* that processing for health research shall involve only aggregate, pseudonymized, or anonymized data. Likewise, all policy and biomedical research related to COVID-19 surveillance and response shall secure an Ethics Board approval prior to implementation.[17]

C. Any authorized further processing shall have adequate safeguards for data privacy and security, such as anonymization, pseudonymization, restriction on access, and shall uphold the rights and freedoms of the data subjects.

SECTION 6. ***Personal data requirements.*** **—** PICs should not collect any unnecessary personal data. Subject to the applicable laws and regulations, the collection of personal data required for the implementation of public health measures, specifically for contact tracing within workplaces and establishments, and the issuance of vaccine cards by either the local government units or the private sector, shall be limited to the following:

A. *Contact tracing forms, whether paper-based or electronic.* Personal data and other details as indicated in the (1) Employee Health Declaration Form and (2) Client/Visitor Contact

[15] See generally: Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (last accessed 29 September 2021).

[16] See: National Privacy Commission, JV v. JR, NPC Case No. 17-047 (August 13, 2019) *available at* https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf

[17] Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (F), (April 24, 2020).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Tracing Form provided for under the Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE) Supplemental Guidelines on Workplace Prevention and Control of COVID-19, Joint Memorandum Circular No. 20-04-A Series of 2020;[18] and

B. *COVID-19 Vaccine Card.* Pursuant to DOH and the National Task Force Against COVID-19 Joint Administrative Order (JAO) No. 2021-0001, a standardized COVID-19 vaccine card shall be issued to vaccine recipients to ensure completion of the required doses by documenting details of their vaccination.[19] The vaccine card shall contain the following information with a template to be issued by the DOH:

1. Basic personal information such as full name, present and/or permanent address, and birthdate;
2. Manufacturer, brand name, batch number, lot number, or other identifier of the COVID-19 vaccine;
3. Date and time of vaccination;
4. Name of the hospital, health center, or health facility where the vaccine was administered;
5. Name, signature, and license number of the duly licensed physician, nurse, pharmacist, midwife or other health worker administering the vaccine;
6. Date of the last RT-PCR testing and the name of the laboratory that conducted the last RT-PCR testing, if applicable;
7. Name and details of contact person or person to be notified, in case of emergency; and,
8. Other information which may be determined as necessary by the Secretary of Health or the IATF-EID.[20]

SECTION 7. ***Privacy Impact Assessment.*** **—** PICs shall conduct a privacy impact assessment (PIA) prior to adoption, use, or implementation of any personal data processing system, such as but not limited to, contact tracing applications (CTAs) and vaccine card systems or applications (Vaccine Card Systems).

A. For existing CTAs and Vaccine Card Systems, a PIA shall be conducted within fifteen (15) days from effectivity of this Circular;

B. A PIA shall be required when there are changes in the governing law or regulations or other proposed modifications which ultimately result in changes to the nature, scope, purpose, manner, and extent of the processing of personal data through CTAs and Vaccine Card Systems; and

C. The submission of the PIA report shall be required by the Commission in case of a compliance check, personal data breach, or investigation. The report shall contain the findings identifying the gaps and risks, how these have been remediated, and the

[18] Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE), Supplemental Guidelines on Workplace Prevention and Control of COVID-19, Joint Memorandum Circular No. 20-04-A Series of 2020 [JMC No. 20-04-A] (Aug 15, 2020).
[19] Department of Health and the National Task Force Against COVID-19, Rules and Regulations Implementing Republic Act No. 11525 [Joint Administrative Order No. 2021-0001], § VII (J) (1), (March 26, 2021).
[20] *Id.* § VII (J) (3).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

status of such remediation efforts.

SECTION 8. ***Privacy Notice.*** **—** PICs shall ensure transparency in all personal data processing activities through an appropriate privacy notice, which is always required regardless of the lawful basis used for the processing. A privacy notice should provide concise, intelligible, and relevant information made readily available to the data subjects.

A. All CTAs and Vaccine Card Systems shall provide the following information through an appropriate privacy notice:

   1. Identity of the PIC;
   2. Description of the personal data to be entered into the system;
   3. Permissions required by applications, including their description and purposes;
   4. Purpose for which the personal data will be processed;
   5. Objective/s that are meant to be achieved by the system;
   6. Lawful basis for processing;
   7. Scope and method of the processing, including:
      a) methods utilized for automated access;
      b) storage and retention period;
      c) policy for destruction or disposal; and
      d) general description of technical security measures and other safeguards;
   8. Recipients to whom personal data are or may be disclosed or shared and the purpose for the same;
   9. The rights of data subjects and how these may be exercised;
   10. Contact details of the data protection officer (DPO); and
   11. Other information that would sufficiently inform the data subject of the nature and extent of data processing involved;

B. Privacy notices shall use clear and plain language. PICs shall determine whether a privacy notice will be more effective if translated into Filipino or in another language or dialect to be better understood by the users;

C. PICs shall convey the privacy notices prior to the collection of data by CTAs and Vaccine Card Systems. PICs shall assess the appropriateness of the contents of the privacy notice vis-à-vis the timing when a privacy notice is displayed through the CTA or Vaccine Card System, e.g., providing information on the specific process that is relevant at a particular time such as at set-up, just-in-time, context-dependent, periodic, persistent, on demand, taking into consideration user experience and the system's interface;

D. For existing CTAs and Vaccine Card Systems, PICs shall notify the data subjects at the next practical opportunity of the information mentioned in subsection A. The timing of the provision of information must always be within a reasonable period to give effect to the data subject's right to be informed; and

E. PICs shall regularly review and update their privacy notice to ensure that it properly reflects the actual processing of personal data for the implementation of public health measures. Where there are changes in the scope, purpose, nature, or extent of the processing, PICs must ensure that the data subjects are adequately informed of the

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

same within a reasonable time: *provided,* that the period shall not exceed thirty (30) business days.

SECTION 9. ***Application (app) permissions.*** **—** Permissions requested by CTAs or Vaccine Card Systems, where applicable, shall be governed by the following:

A. *Request minimum permissions*. PICs shall assess the proportionality of app permissions and only request for those that are necessary to fulfill its functions.

B. *Ask in context.* Apps requiring specific permissions shall request them at the most reasonable and appropriate time, such as by means of pop-up notices or just-in-time notices, or any similar manner when the app or the data subject's use requires or triggers it.[21]

C. *Provide adequate user choices.* Whenever possible, apps shall minimize the time or access window of permissions and provide clear choices to users in managing permissions:

1. While using the app. The app will only have access to the specific permission when the app is being actively used in the foreground or in the active window of the device;
2. Only this time. The app will have access temporarily to a specific permission sought from the user, i.e., one-time permission, where such permission shall automatically be withdrawn after the app is closed by the user; and
3. Deny. The app will be prohibited to use the requested permission. PICs are required to provide mechanisms whereby users are still able to use the app despite this choice.

D. *Only access sensitive permissions when necessary and the user reasonably expects it.* Apps must provide continuous visual cues, indicators, or notices that are easily understood by users, such as a small icon in the status bar for mobile phones or in the browser's toolbar for websites, that applications are actively accessing sensitive permissions, i.e., camera, location, microphone.

E. *Pay attention to libraries.* Apps shall be audited with regard to personal data especially sensitive personal information accessed by third-party Application Programming Interfaces (APIs) and libraries. Such third-party APIs and libraries must also be clearly indicated in the app's privacy notice.

SECTION 10. ***Security Measures.*** **—** PICs shall implement adequate safeguards to protect personal data processed against accidental, unlawful, or unauthorized use or access.[22]

A. *Technical measures.* PICs shall integrate privacy by design and secure software development at every stage of the lifecycle to ensure the protection of personal data that will be processed without diminishing functionality. PICs shall consider the following recommended measures:

[21] See: National Privacy Commission, ECA v. XXX, NPC 18-103 (July 23, 2020) *available at* https://www.privacy.gov.ph/wp-content/uploads/2020/12/NPC-18-103-ECA-v-XXX-Decision-ADJU1.pdf.
[22] Data Privacy Act of 2012, § 20 (2012).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

1. *Requirements.* PICs shall determine the appropriate requirements for the CTAs and Vaccine Card Systems including, but not limited to, the types and amount of personal data to be processed, the minimum application permissions required, policies in using the personal data, system architecture, threat modeling, and programming code or language to be used.

    a) The requirements should comply with the general data privacy principles of transparency, legitimate purpose, and proportionality.
    b) PICs shall also inform the data subjects of the risks posed by the system's architecture based on the results of the threat modeling and privacy impact assessment activities.

2. *Good practices.* PICs shall ensure that both digital and manual contact tracing or processing for vaccine deployment are configured securely.

    a) PICs shall deploy up-to-date software components and ensure the secure configuration thereof to mitigate the risk of personal data disclosure. Likewise, PICs shall follow good practices in developing and managing the application based on industry standards, such as secure coding principles, secure design principles, and the conduct of essential software testing.
    b) For manual contact tracing or processing for vaccine deployment, PICs shall provide individual forms for the data subjects to accomplish. The use of logbooks that aggregates all their information in a single page shall be prohibited.
    c) Access controls must be in place to protect physical contact tracing forms from accidental or unauthorized disclosure.

3. *Risk Management.* PICs shall determine and implement appropriate risk management strategies in conducting assessments in identifying risk, threats, and vulnerabilities on the development and implementation of CTAs and Vaccine Card Systems;

4. *Encryption.* Personal data at rest shall be encrypted. All network communications between the application and the backend shall be encrypted. For this purpose, the Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard. PICs shall also use transport layer encryption to encrypt data in transit when communicating over mobile and Wi-Fi networks;

5. *Tests.* PICs shall test the application as the need arises, such as when there are new updates on the app or its components. For this purpose, PICs shall use both automatic and manual methods to check for any weak configurations, which may unintendedly expose personal data, endpoints, and other components that are not meant to be accessible. Testing should not be limited to functional tests but also security tests such as vulnerability scanning, code quality checks, (static and dynamic) code analysis tools, and source code scanning for libraries and developed code; and

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

6. *Information Security Incident Management Policy.* PICs shall implement policies and procedures for managing security incidents in accordance with NPC Circular No. 16-03.[23] The policies and procedures shall contain a process for assessing reasonably foreseeable vulnerabilities in computer networks as well as identifying the preventive, corrective, and mitigating action necessary against incidents that can lead to a personal data breach.

B. *Access.* PICs shall implement an access control policy that shall identify and limit the personnel who shall be authorized to have access to the personal data collected through CTAs and Vaccine Card Systems, taking into account the applicable DOH issuances on the matter, i.e., only concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be allowed to access health information in relation to COVID-19 cases and/or identified close contacts.[24]

   1. Authorized personnel shall be adequately trained on the proper processes in handling personal data collected and shall be required to execute a non-disclosure agreement (NDA); and
   2. PICs shall be responsible for ensuring that their authorized personnel strictly abide by the provisions of the DPA, its IRR, and related issuances. PICs shall also remind its authorized personnel and the third-party service providers that processing the collected personal data for any other purpose is punishable under the DPA.

C. *Disclosure.* Disclosure of the personal data collected through the CTAs and Vaccine Card Systems shall be limited to public health authorities, such as the DOH and its authorized partner agencies, LGUs, or other lawfully authorized entities, officers, or personnel, and must only be for the purpose of responding to the public health emergency.

   In complying with the reportorial requirements of existing regulations, all PICs shall ensure that the same are securely transmitted, and must consider the following:

   1. Keep records of all submissions/transmittals for reportorial requirements;
   2. Implement procedures to verify the genuineness of any information request made for contact tracing and vaccination status, and the response procedure for such verified request;
   3. Ensure strict compliance with the protocols established by the DOH and LGUs for disclosing information through the conduct of contact tracing of those in close contact with a COVID-19 case;
   4. Refer individuals for quarantine, isolation, testing, clinical management, etc. shall be in accordance with DOH guidelines;[25]
   5. Disclosure of personal data to the public, the media, or any other public-facing

[23] National Privacy Commission, Personal Data Breach Management [NPC Circular No. 2016-03] (December 15, 2016).
[24] Department of Health (DOH) and National Privacy Commission (NPC), Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (C), (April 24, 2020).
[25] See generally: Department of Health, Omnibus Interim Guidelines on Prevention, Detection, Isolation Treatment, and Reintegration Strategies for COVID-19 [Department Memorandum No. 2020-0439] (Oct 6, 2020).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

platforms without the consent of the patient or vaccinee or his/her authorized representative or next of kin, shall be strictly prohibited.

SECTION 11. ***Mandatory Submission of List of CTAs and Vaccine Card Systems.*** **—** PICs shall submit to the Commission a complete list of all the CTAs and Vaccine Card Systems which they operate. The procedure for registration shall be in accordance with the relevant NPC issuances.

SECTION 12. ***Storage and Retention.*** **—** All personal data collected through CTAs and Vaccine Card Systems shall be stored in a secure manner using appropriate measures, including encryption. Personal data shall be retained only for as long as necessary when the purpose for processing still exists and in accordance with the period allowed by existing government issuances.

A. Generally, personal data collected through CTAs shall be stored only for a limited period and shall be disposed of properly after thirty (30) days from date of collection.[26] For CTAs involving the use of unique Quick Response (QR) Codes which are assigned to specific individuals or other similar systems, PICs shall distinguish the personal data or records for purposes of determining the retention period:

    1. Names, addresses, and mobile numbers may be retained for a longer period or for as long as there is a state of public health emergency necessitating the need for such system; and
    2. Records of the date, time, and location when and where the QR code was scanned, body temperature readings, and other health declaration details should be routinely disposed of after thirty (30) days.[27]

B. The retention period for Vaccine Card Systems and the DOH central database of vaccinations shall be governed by the appropriate law or DOH regulation on the matter.[28]

SECTION 13. ***Disposal of personal data and decommissioning of CTAs and Vaccine Card Systems.*** **—** Policies on disposal and decommissioning shall be implemented by all PICs.

A. Personal data collected through CTAs and Vaccine Card Systems shall be disposed in a proper and secure manner after the appropriate retention period, such that further processing is no longer possible. PICs shall implement a disposal policy considering industry standards for disposal procedures ensuring that personal data are permanently and irreversibly destroyed; and

B. PICs shall ensure the deactivation or decommissioning of CTAs and Vaccine Card Systems within a reasonable period after the state of public health emergency has been

[26] See: DTI-DOLE JMC No. 20-04-A, § Sections II.D.I.e.v and III.C.4.d.
[27] See: National Privacy Commission, NPC Advisory Opinion No. 2020-054 (Dec. 28, 2020).
[28] See: Department of Health, The Revised Disposition Schedule of Medical Records Amending Ministry Circular 77, s. 1981 [Department Circular No. 70, s.1996] (May 8, 1996) available at https://zcwdv320190208-dot-efoi-ph.appspot.com/requests/aglzfmVmb2ktcGhyHQsSB0NvbnRlbnQiEERPSC0yNDIzOTEyNzUzMDIM; Department of Health National Center for Health Facility Development, Hospital Health Information Management Manual (2010) available at http://ehealth.doh.gov.ph/nehehrsv/sys/assets/HOSPITAL%20HEALTH%20INFORMATION%20MANAGEMENT%20MANUAL%20formerly%20HOSPITAL%20MEDICAL%20RECORDS%20MANAGEMENT%20MANUAL.pdf.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

lifted, adopting applicable industry standards. CTAs or Vaccine Card Systems shall not be repurposed unless otherwise provided by law and subject to the condition that all categories of personal data previously collected and stored for contact tracing and vaccine deployment are properly disposed of.

SECTION 14. ***Data subject rights.*** **—** CTAs and Vaccine Card Systems shall provide adequate user controls in the form of a dedicated privacy control panel, dashboard, or similar interface that enables the exercise of data subject rights under the DPA.

SECTION 15. ***Penalties.*** **—** The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liabilities pursuant to the provisions of the DPA, related issuances of the NPC, and other applicable laws and regulations.

SECTION 16. ***Interpretation***. **—** Any doubt in the interpretation of any provision of this Circular shall be liberally interpreted in a manner mindful of the rights and interests of the data subject.

SECTION 17. ***Transitory provision.*** **—** Within fifteen (15) days from the effectivity of this Circular, all PICs shall register their DPOs and submit to the Commission a complete list of all the CTAs and Vaccine Card Systems that they operate in accordance with existing rules on NPC registration under NPC Circular No. 17-01. Within the same period, PICs shall conduct a mandatory review of all personal data processing systems related to the response to public health emergencies to determine compliance of such systems with the provisions of this Circular.

SECTION 18. ***Separability Clause.*** **—** If any portion or provision of this Circular is declared invalid or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 19. ***Repealing Clause.*** **—** All issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 20. ***Effectivity.*** **—** This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or two newspapers of general circulation.

Approved:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228