Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2020 - 03

DATE : 23 October 2020

SUBJECT : GUIDELINES FOR WORKPLACES AND ESTABLISHMENTS PROCESSING PERSONAL DATA FOR COVID-19 RESPONSE

SECTION 1. ***Rationale.*** – This Advisory aims to provide additional guidance to supplement the Joint Memorandum Circular (JMC) No. 20-04-A Series of 2020[1] issued by the Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE) which requires workplaces and various establishments to collect employee health declaration forms and client/visitor contact tracing forms, and implement measures to manage asymptomatic and symptomatic employees in the workplace.

SECTION 2. ***Establishments as personal information controllers (PICs).*** – Subject to any amendments of the above JMC and the role of establishments in relation to the implementation of contact tracing, establishments implementing the above JMC are considered as PICs as they control the processing of personal and sensitive personal information (collectively, personal data) of their employees, clients/customers, and visitors.

As PICs, they are required to comply with the provisions of the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other issuances of the National Privacy Commission (NPC), which includes respecting and upholding data subject rights.

SECTION 3. ***Processing personal data for COVID-19 prevention and control.*** – Processing personal data pursuant to or as may be required under a law or regulation to support the government's COVID-19 response is allowed under the DPA.

To ensure the protection of personal data, establishments shall adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality, implement reasonable and appropriate security measures at each stage of the personal data lifecycle, and uphold data subject rights.

SECTION 4. ***Ensuring fairness and lawfulness in processing.*** – Establishments shall collect personal data only for purposes of the COVID-19 prevention and control, specifically on activities such as contact tracing and managing asymptomatic and symptomatic employees in the workplaces.

A. Establishments shall limit the collection of information to those purposes which are

[1] 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] (15 Aug 2020).

required for COVID-19 prevention and control based on existing government issuances: (1) Employee Health Declaration Form, (2) Client / Visitor Contact Tracing Form; and (3) Customer Information and Health Checklist. [2]

B. The employees, clients/customers, and visitors of the establishments must be informed through a privacy notice of the details of the processing of their personal data for COVID-19 prevention and control. Such privacy notice shall be easy to access and understand, using clear and plain language.

    1. The privacy notice must be visible within the premises or establishment where the data are collected, such as points of entry and other conspicuous areas.

    2. If personal data is collected through electronic means, establishments shall ensure that the privacy notice is displayed in a way that a reasonable person would be able to immediately notice and access it, e. g. when QR codes are used, the privacy notice should be posted beside the QR code with the contact number of the data protection officer of the establishment.

    3. The following information must be included in the privacy notice:

        a) description of the personal data to be entered into the system, which includes an enumeration of the type of personal data that will be processed;
        b) purpose(s) for which they will be processed, which should only be for contact tracing and management of asymptomatic and symptomatic employees in the workplace;
        c) basis for processing which are the existing laws and regulations, specifically the DTI, DOLE, and Department of Health (DOH)-issued guidelines requiring the accomplishment of the health declaration forms for employees, contact tracing forms for visitors and customer information and checklist form for clients.[3]
        d) scope and method of the personal data processing, which should discuss how the data will be used, stored, protected, and eventually disposed;
        e) recipients to whom data may be disclosed, such as the DOH and its partner agencies, local government units (LGUs) or other authorized persons, including the reason for such disclosure, i.e., conduct effective contact tracing, assist the government in providing effective response during the COVID-19 pandemic;
        f) methods used for automated access by the recipient, and its expected consequences to the data subjects;
        g) identity and contact details of the personal information controller, including the contact information of the data protection officer;
        h) the duration for which data will be kept, which shall be for thirty (30) days for data collected through the employee health declaration form and client/visitor contact tracing form;[4] and
        i) the existence of rights available to the data subjects under the DPA,

[2] See: DTI-DOLE JMC No. 20-04, Annex A-1: Employee Health Declaration Form and Annex A-2: Client /Visitor Contact Tracing Form; DTI Memorandum Circular 20-37, Guidelines on the Minimum Health Protocols for Dine in Services by Restaurants and Fastfood Establishments; and Updated Guidelines for Barbershops and Salons Pursuant to IATF Resolution No. 51 Series of 2020, Amending for the Purpose DTI Memorandum Circular No. 20-28, Series of 2020, Annex A: Customer Information and Health Checklist of Annex A: Customer Information and Health Checklist of DTI Memorandum Circular 20-38.
[3] *Id.*
[4] DTI-DOLE JMC No. 20-04-A, § II.D.I.e.v and III.C.4.d.

including how the employees, customers or visitors can exercise their data subject rights through an appropriate channel or procedure within the establishment.

4. For further information on the processing activity, establishments may direct their employees, clients/customers, and visitors to their official websites or social media pages, as well as official websites of the pertinent government agencies.

5. If the employees, customers, or visitors request that the details be explained or discussed to them, the establishment must be able to do so through its authorized personnel.

C. To ensure data quality and accuracy, the security personnel or other authorized personnel shall make sure that:

1. The personal data submitted is accurate and legible. All required fields must be filled out. Upon reasonable belief that the information provided is wrong, they can ask the employee, client/customer, or visitor for correction and/or clarification in such a way that the confidentiality of the data being shared is preserved (i.e., avoiding other persons nearby from hearing the conversation).

2. Subject to the requirements of the immediately preceding provision, identity checks shall not be undertaken nor any other intrusive means of gathering personal data, unless the same is part of a documented regular procedure, such as presentation of company ID for employees or asking for proof of identity for visitors.

3. The date and time of shift (for the Employee Health Declaration Form) or the date and time of visit (for the Client/Visitor Contact Tracing Form) are correctly written.

E. Repurposing the personal data collected for direct marketing, profiling, or any other use or purpose, whether commercial or non-commercial, is prohibited.

F. Establishments shall be responsible for reminding their employees and third-party service providers, such as security personnel, that using the collected personal data of employees, customers, or visitors for any other purpose is punishable under the DPA.

SECTION 5. ***General guidelines.*** **–** The following guidelines are provided to ensure the implementation of reasonable and appropriate safeguards in the processing of personal data for the COVID-19 response.

A. *Collection of personal data through physical or electronic forms.* Establishments may collect personal data and other information manually through paper-based forms or electronically through digital or online forms. The following shall be considered:

1. Establishments must provide a designated area where employees and clients/visitors can accomplish the forms with the observance of physical distancing measures. At the same time, physical distancing provides additional protection by eliminating the risk of shoulder surfing or data

exposure among employees and clients/visitors.

2. Where Quick Response (QR) codes are used, an employer may assign each of its personnel a unique QR code which, when scanned upon entry, shall automatically log the entry into the online employee health declaration form.

   For Clients /Visitors, QR codes posted in the entrance of the establishment may be used. Such codes, when scanned by a mobile phone camera, shall link to an electronic web form to be filled out by clients visiting the premises.

3. Security personnel or other authorized personnel must safeguard the Employee Health Declaration and Client/Visitor Contact Tracing Forms, and ensure that:

   a) Paper- based systems:

      1. Paper-based systems shall refer to logbooks, folders, individual forms, notepads, and such other modes of collecting and processing personal information on any kind of paper.
      2. To prevent data breach, the use of open access, paper-based systems where personal information is visible and accessible to others shall be prohibited. However, paper-based systems that have reasonable and appropriate safeguards and are not openly accessible to the public or other data subjects may be allowed.
      3. Accomplished forms are kept physically segregated to prevent unintended disclosure of personal data.
      4. Only the designated or authorized personnel shall receive and have access to the accomplished forms.
      5. The body temperature of an employee, client, or visitor is recorded correctly, following the establishments' protocol for temperature check.
      6. All accomplished forms are transmitted to the authorized personnel/unit within the establishment for appropriate action and storage at the end of the day or as may be prescribed by the internal policies on the matter. The transmittal of the forms shall be done in such a way that the confidentiality, integrity, and availability of the data is preserved.

   b) Digital forms:

      1. Encryption in storing and transmitting personal data from the digital platform is implemented.
      2. Electronic forms have adequate safeguards against any intentional breach.
      3. Electronic forms are correctly and properly completed by adding field validation (e.g. making each field required to ensure the completeness and integrity of the information provided).
      4. Should establishments make available their electronic devices (i.e. smartphones or tablets) for public use in their data entry, the following must be complied with:

i. The device's operating system and security patches are kept up to date.
ii. The web browser's autofill or autocomplete feature is disabled to prevent other users from seeing information previously entered in the electronic form.
iii. The device is regularly scanned using the latest virus signature definitions for viruses and malware.
iv. Access is limited to authorized personnel. The electronic devices deployed must be enabled with an automatic lock feature, encrypted with a password or protected with biometrics for login and equipped with a remote wipe functionality, whenever practical, so that data are securely deleted should the device be reported lost or stolen.

B. *Collection of personal data through other means.* Establishments may collect the data of employees, clients, customers, and visitors, as well as the data of close contacts through COVID-19 testing registration forms, quarantine reports, CCTVs, and other similar means. All forms collected or all information required to be submitted for monitoring during quarantine shall be appropriately secured.

Access to and use of personal data collected through CCTVs shall likewise be subject to the guidelines and requirements as may be provided in a separate Advisory to be issued by the NPC.

C. *Use of the personal data collected.* All establishments shall ensure that the personal data collected are used only for the purpose of contact-tracing measures and the management of asymptomatic and symptomatic employees in the workplace.

1. Policies and procedures shall be implemented to determine any close contacts of a probable or confirmed COVID-19 case within the establishment. Such policies shall take into consideration the data privacy rights of the employees, clients/customers, and visitors. In no case shall the identity of the suspect, probable, or confirmed case be disclosed to other employees, clients/customers, or visitors as there are less privacy-intrusive means of determining close contacts and conducting contact tracing.

2. To address apprehensions on the safety of the workplace, the risk of reporting for work, and to avoid disclosing the identity of any probable or confirmed case, the establishment, through the Human Resources or Safety Officer, shall pseudonymize data on any probable or confirmed cases. This may enable information sharing and/or data analysis in the conduct of contact tracing without disclosing the identities of the probable or confirmed cases.

3. The following documents and sources of information may be reviewed to determine the close contacts:

a) Attendance records;
b) CCTV footages;
c) Calendar of meetings;
d) Client/Visitor Contact Tracing Form;
e) Employee Daily Health Declaration Form; or

f) Logbooks in facilities of exposure (cafeterias, shuttle services, locker rooms, sleeping quarters, production floor, comfort rooms, etc.).

4. In the conduct of interviews to determine close contacts, the interviewees shall be informed on the purpose, scope, and extent of the processing of personal data involved in the contact tracing activity.

5. Employers are encouraged to collaborate with the national and/or local government testing efforts like drive-thru or walk-thru testing facilities.[5] If collaboration is made, the employers must make sure that the employees are duly informed of the following:

   a) The national and/or local government testing facilities that will be given access to their personal data;
   b) Purpose of data sharing which should only be to effectuate the COVID-19 testing activity;
   c) Categories of personal data concerned;
   d) Existence of the rights of data subjects and how they can exercise them;
   e) Other information that would sufficiently notify the employee of the nature and extent of data sharing and the manner of processing.

6. Symptomatic employees should update their employer regarding their COVID-19 test results from a nationally accredited testing facility.[6] The employer must make sure that the data collected through reports submitted by their employees are properly collected, stored and used only for contact tracing and preventing and managing the spread of the disease in the workplace, including coordination with the nearest health care facility to refer the symptomatic employee as provided under the existing DOH guidelines.[7]

7. Employers shall inform the LGU/s having jurisdiction over the workplace and the respective residence/s of the symptomatic employees and close contacts before testing for monitoring purposes.[8] In this case, employers must ensure that the employee's personal data is securely shared or transferred and must ensure that the same is disclosed only to the proper authorities.

E. *Storage and retention.* Personal data collected shall be retained only for as long as necessary for the fulfillment of the purpose/s for which such personal data was obtained.

1. Authorized personnel shall ensure that the physical Employee Health Declaration Forms and Client/Visitor Contact Tracing Forms, COVID testing registration forms, quarantine reports and other pertinent documents and information are kept in a secure place at the end of business hours (e.g. stored in a locked cabinet or drawer). Only authorized personnel shall have access to the same. Digital forms shall be secured using the appropriate measures,

[5] DTI-DOLE JMC No. 20-04-A, § III.D.3.a.
[6] *Id.* § III.C.3.b and d.
[7] See: Department of Health, Strategies in Health Facility Coordination in line with Department Memorandum No. 2020-0178 entitled "Interim Guidelines on Health Care Provider Network during the COVID-19 Pandemic, Department Memorandum 2020-0334 (17 July 2020).
[8] DTI-DOLE JMC No. 20-04-A, § III.D.3.a.

including encryption.

2. Establishments shall implement an access control policy which shall identify and limit the personnel who shall be authorized to have access to the personal data collected for the COVID-19 response. These authorized personnel shall be adequately instructed on the proper processes in handling these forms, whether physical or digital, and other information, and may be required to execute a non-disclosure agreement.

3. Establishments shall be prepared to restore the availability and access to personal data in a timely manner in case of a physical or technical incident through the implementation of the necessary policies, i.e. backup policy and procedure.

4. Safeguards to protect computer networks or physical records against accidental, unlawful or unauthorized use or access shall be ensured by having the appropriate policies in place, i.e. Network Policy, Information Technology Policy, Information Security Policy, Bring You Own Device (BYOD) Policy, etc.

5. Adopting an Information Security Incident Management Policy containing procedures for the regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in computer networks and physical files, and likewise identifying the preventive, corrective, and mitigating action necessary against incidents that can lead to a personal data breach is recommended.

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.[9]

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.

F. *Disclosure or sharing*. Disclosure of the personal data collected through the health declaration form or other similar or related forms shall be limited to DOH and its partner agencies, LGUs, or authorized entities, officers or personnel, and must only be for the purpose of conducting contact tracing or the management of probable, suspected and confirmed COVID-19 patients.

1. In complying with the reportorial requirements of existing regulations, all PICs shall ensure that the same are securely transmitted, and must take in consideration the following measures:

    a) Workplaces and establishments shall keep records of all submissions/ transmittals of reportorial requirements.

[9] DTI-DOLE JMC No. 20-04-A, § Sections II.D.I.e.v and III.C.4.d.

b) Comply with existing government regulations such as:

1. Reporting of COVID-19 test results to the DOH which should be done in accordance with DOH Administrative Order No. 2020-0013, entitled "Revised Guidelines for the Inclusion of COVID-19 in the List of Notifiable Diseases for Mandatory Reporting to the Department of Health."

2. Reporting of COVID-19 positive employees, symptomatic employees, and their close contacts, by the Occupational Safety and Health Officer/employer to the local health office having jurisdiction over the workplace and the Barangay Health Emergency Team (BHERT) of their place of residence, in accordance with DOH DM No. 2020-0189.

3. Monthly reporting to the DOLE through its Regional Office copy furnished DOH of illness, diseases and injuries in accordance with Section X of the DTI-DOLE Interim Guidelines on Workplace Prevention and Control of COVID-19 using the Work Accident/Illness Report (WAIR) COVID-19 form.

c) The establishment or workplace must have procedures in place to verify the genuineness of any request made by an alleged contact tracing team. The staff or personnel tasked to provide the details of individuals in response to such verified request should know which unit or personnel to direct the contact tracing team.

d) Disclosure of a patient's personal data to the public, the media, or any other public-facing platforms without the written consent of the said patient or his/her authorized representative or next of kin, shall be strictly prohibited.[10]

e) Establishments must 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 COVID 19 case.[11]

f) Referral of symptomatic individuals shall be coordinated to the nearest health care facility as provided under the latest DOH interim guidelines.[12]

G. *Disposal or destruction*. The personal data shall be disposed in a secure manner after the required retention period discussed above. Paper records must be shredded properly while storage media of the digital devices must be electronically wiped, including back up data, to ensure that stored personal data are beyond recovery. A Data Disposal Policy shall be implemented accordingly.

SECTION 6. ***Data subject rights***. — The rights and redresses under the DPA are available to the employees, clients/customers, visitors, and their close contacts. Establishments and

[10] Department of Health and National Privacy Commission, Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response, Joint Memorandum Circular No. 2020-0002, § VI (D) (2) (a) (24 April 2020).
[11] *See generally:* DOH NPC JMC No. 2020-0002 and DOH DM No. 2020-0189.
[12] See *supra* note 7.

workplaces are bound to uphold data subject rights.

Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subject.

Approved:

SGD.
RAYMUND E. LIBORO
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner