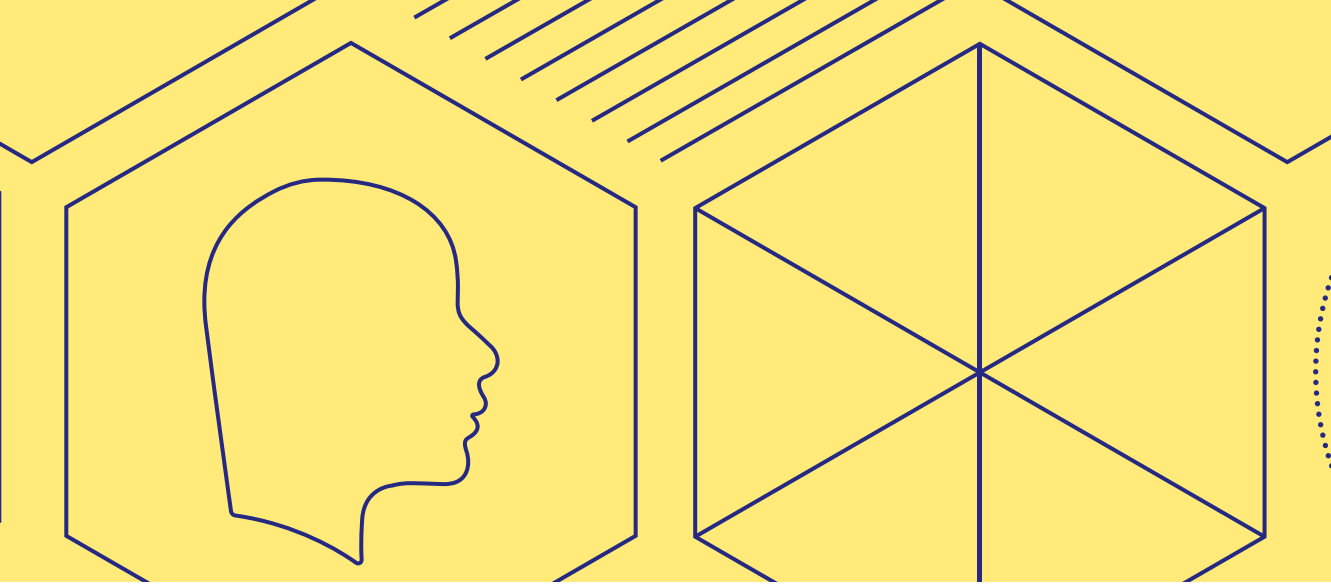


NATIONAL PRIVACY COMMISSION

THE 2018 COMPENDIUM of NPC ISSUANCES

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

MESSAGE

The National Privacy Commission's 2018 Compendium of Issuances is a collection of 75 Advisory Opinions, 3 Circulars, 1 Advisory, and 3 Commission-issued Orders. This is made available to the public to serve as a ready reference for dedicated Data Protection Officers, privacy advocates, students of privacy and anyone keenly interested in data protection issues and privacy governance.

The compendium delves into a variety of concerns such as: regulation, data protection, privacy rights, vulnerability, and risk management, among others. While they are not in any way aimed to serve as the final word in data privacy discourse, they serve as guideposts towards the aim of protecting personal data privacy, especially in an era of the data-driven economy, when the rise of technology has made such a goal an imperative.

Effective adaptation to the challenges of this era rests heavily on the shoulders of decision makers, privacy workers, and allied professionals. Having a copy of the NPC's annually-issued compendium would help them remain current and responsive to the dynamic pace of development in the field. This should also enable them to increase their knowledge and be adaptive amid the continuously evolving threats to people's data privacy rights.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

TABLE OF CONTENTS

03 **NPC MEMORANDUM CIRCULARS**

04 **NPC CIRCULAR NO. 18-01**
Rules of Procedure on Requests for Advisory Opinions

05 **RULE I. PRELIMINARY PROVISIONS**
Section 1. General Principles
Section 2. Advisory Opinion
Section 3. Scope and Coverage

06 **RULE II. REQUIREMENTS FOR REQUESTS FOR ADVISORY OPINIONS**
Section 4. Letter Request
Section 5. Subject of an advisory opinion
Section 6. Supporting documents
Section 7. Withdrawal of a request
Section 8. Filing as a complaint
Section 9. Conference with the Requesting Party

08 **RULE III. GENERAL PROVISIONS**
Section 10. Letter Request
Section 11. Subject of an advisory opinion
Section 12. Supporting documents
Section 13. Withdrawal of a request
Section 14. Filing as a complaint

10 **NPC CIRCULAR NO. 18-02**
Guidelines on Compliance Checks

12 **RULE I. GENERAL PROVISIONS**
Section 1. Scope
Section 2. Purpose
Section 3. Definition of Terms

14 **RULE II. GUIDELINES FOR THE CONDUCT OF COMPLIANCE CHECK**
Section 4. Modes of Compliance Checks
Section 5. Considerations for the Conduct of Compliance Checks
Section 6. When to Conduct Compliance Check
Section 7. Notice of Compliance Checks

Section 8. Issuance of Notice of Deficiencies
Section 9. Issuance of Compliance Order
Section 10. Issuance of Other Orders
Section 11. Certificate of No Significant Findings
Section 12. Failure to Comply with Compliance Order
Section 13. Refusal to Undergo Compliance Check
Section 14. Fines and Penalties

18 **RULE III. MISCELLANEOUS PROVISIONS**
Section 15. Publication
Section 16. Separability Clause
Section 17. Effectivity Clause

20 **NPC CIRCULAR NO. 18-03**
Rules on Mediation before the National Privacy Commission

21 **RULE I. PRELIMINARY PROVISIONS**
Section 1. Application and Interpretation
Section 2. Scope
Section 3. Definition of Terms

22 **RULE II. PROCEDURE**
Section 1. Willingness to Mediate
Section 2. Application for Mediation
Section 3. Order to Mediate
Section 4. Preliminary Mediation Conference
Section 5. Separate Caucuses and Subsequent Conferences
Section 6. Mediation Period and Extension thereof
Section 7. Mediated Settlement Agreement
Section 8. Confirmation by the Commission
Section 9. Effect of Confirmed Mediated Settlement Agreement
Section 10. Failure to Reach Settlement
Section 11. Resumption of Complaint Proceedings
Section 12. Field Mediation

24 **RULE III. GENERAL PROVISIONS**
Section 1. Personal Appearance by the Parties
Section 2. Effect of Failure of Parties to Appear
Section 3. Presence of Lawyers in Mediation
Section 4. Venue
Section 5. Confidentiality
Section 6. Mediation Fees

26 **RULE IV. MISCELLANEOUS PROVISIONS**
Section 1. Amendments
Section 2. Separability Clause
Section 3. Transitory Provision
Section 4. Effectivity

37 NPC ADVISORIES

38 NPC ADVISORY NO. 18-02
Updated Templates on Security Incident and Personal Data Breach Reportorial Requirements

47 NPC ADVISORY OPINIONS

48 Advisory Opinion No. 2018-001
REQUEST FOR OPINION ON THE APPLICABILITY OF THE DATA PRIVACY ACT OF 2012 ON CONTRACTS

51 Advisory Opinion No. 2018-002
COMMISSION ON AUDIT (COA) REQUEST FOR ACCESS TO BANGKO SENTRAL NG PILIPINAS (BSP) EMPLOYEES' DIRECTORY

55 Advisory Opinion No. 2018-003
VISITOR LOGBOOK

58 Advisory Opinion No. 2018-004
EMPLOYEE NON-DISCLOSURE UNDERTAKING

61 Advisory Opinion No. 2018-005
DATA SHARING AGREEMENT/ DATA PROTECTION OFFICER

64 Advisory Opinion No. 2018-006
CONSENT OF DATA SUBJECT PRIOR TO RELEASE OF SCHOOL RECORDS BY THE LYCEUM OF THE PHILIPPINES UNIVERSITY (LPU)

66 Advisory Opinion No. 2018-007
DISCLOSURE OF THE MASTER LIST OF STUDENTS AND INDIVIDUALS WHO WERE VACCINATED WITH DENGVAXIA

69 Advisory Opinion No. 2018-008
SUBMISSION OF EMPLOYEE NAMES AND SALARY RECEIVED IN CY 2017 FOR ISSUANCE OF COMMUNITY TAX CERTIFICATE (CTC)

72 Advisory Opinion No. 2018-009
DISCLOSURE OF PERSONAL INFORMATION TO THE PHILIPPINE ARMY

75 Advisory Opinion No. 2018-010
PRECINCT FINDER AND COMELEC MINUTE RESOLUTION NO. 17-0715

78 **Advisory Opinion No. 2018-011**
DISCLOSURE OF THE UNIT NUMBERS OF THE MEMBERS OF A CONDOMINIUM ASSOCIATION

81 **Advisory Opinion No. 2018-012**
RELEASE OF SERVICE RECORD

83 **Advisory Opinion No. 2018-013**
PRIVACY POLICY AND CONSENT OF DATA SUBJECTS

87 **Advisory Opinion No. 2018-015**
CONSENT REQUIREMENT ON OUTSOURCING AGREEMENT WITH AN EXTERNAL SERVICE PROVIDER

90 **Advisory Opinion No. 2018-016**
COMPLIANCE OF RESIDENT PHYSICIANS TO THE REQUIREMENT OF PROFESSIONAL SOCIETIES FOR DIPLOMATE BOARD EXAM AND ACCREDITATION

93 **Advisory Opinion No. 2018-017**
TRADE SECRETS

95 **Advisory Opinion No. 2018-018**
PUBLICATION OF DECISIONS ON PHILHEALTH WEBSITE

98 **Advisory Opinion No. 2018-019**
APPOINTMENT OF DATA PROTECTION OFFICER AND REGISTRATION OF DATA PROCESSING SYSTEM OF A HOMEOWNERS' ASSOCIATION (HOA)

101 **Advisory Opinion No. 2018-020**
POSTING OF THE LIST OF ADMITTED STUDENTS ON THE BULLETIN BOARD OF THE SCHOOL

104 **Advisory Opinion No. 2018-021**
TELEPHONE DIRECTORIES

107 **Advisory Opinion No. 2018-022**
SCOPE AND COVERAGE OF THE DATA PRIVACY ACT

110 **Advisory Opinion No. 2018-024**
REPORTING OF ALLEGED CRIMINALS' PERSONAL DATA

115 **Advisory Opinion No. 2018-025**
REQUEST FOR INFORMATION FROM LAW ENFORCEMENT AGENCIES

118 **Advisory Opinion No. 2018-026**
LAWFUL PROCESSING OF PERSONAL DATA

120 **Advisory Opinion No. 2018-027**
PASIG CITY ORDINANCE NO. 11 "AN ORDINANCE REQUIRING THE REGISTRATION OF MIGRANTS, TENANTS, BOARDERS AND TRANSIENTS TO THE BARANGAY, AND FOR OTHER PURPOSES"

125 **Advisory Opinion No. 2018-028**
OWNERSHIP OF 201 FILES

128 **Advisory Opinion No. 2018-029**
PSEUDONYMIZATION OF PERSONAL AND SENSITIVE PERSONAL INFORMATION

131 **Advisory Opinion No. 2018-030**
REQUEST FOR COMELEC TO COLLECT AND PUBLISH DATA ON WOMEN AND DIFFERENTLY-GENDERED CANDIDATES AND ELECTED OFFICIALS

135 **Advisory Opinion No. 2018-031**
PRIVACY NOTICE

139 **Advisory Opinion No. 2018-032**
PPP CENTER PRIVACY MANUAL

143 **Advisory Opinion No. 2018-033**
DATA SHARING, CONSENT, AND COMPLIANCE WITH THE DATA PRIVACY ACT OF 2012

148 **Advisory Opinion No. 2018-034**
BUREAU OF INTERNAL REVENUE REQUEST FOR INFORMATION

151 **Advisory Opinion No. 2018-035**
CERTIFIED LIST OF DECEASED PERSONS REQUIRED UNDER REPUBLIC ACT NO. 8189

153 **Advisory Opinion No. 2018-036**
CERTIFIED LIST OF DECEASED PERSONS REQUIRED UNDER REPUBLIC ACT NO. 8189

157 **Advisory Opinion No. 2018-037**
CERTIFIED LIST OF DECEASED PERSONS REQUIRED UNDER REPUBLIC ACT NO. 8189

161 **Advisory Opinion No. 2018-038**
PERSONAL INFORMATION CONTROLLER IN THE PROCESSING OF CONCESSIONARY BEEP™ CARDS

164 **Advisory Opinion No. 2018-039**
RIGHT TO ERASURE IN RELATION TO RETENTION OF PERSONAL INFORMATION

168 **Advisory Opinion No. 2018-040**
PUBLICATION OF NAMES OF SANCTIONED DIRECTORS AND OFFICERS OF BSP-SUPERVISED FINANCIAL INSTITUTIONS

171 **Advisory Opinion No. 2018-041**
PASIG CITY ORDINANCE NO. 51

175 **Advisory Opinion No. 2018-042**
EMPLOYEE'S RIGHT TO ACCESS EMPLOYMENT

179 **Advisory Opinion No. 2018-043**
REGISTRATION OF DATA PROCESSING SYSTEMS

182 **Advisory Opinion No. 2018-044**
REQUEST FOR INFORMATION FROM RIZAL MEDICAL CENTER

190 **Advisory Opinion No. 2018-045**
RIGHT TO ACCESS CLINICAL INFORMATION OF PATIENTS

193 **Advisory Opinion No. 2018-046**
CONSENT FOR BUSINESS CORRESPONDENCE

196 **Advisory Opinion No. 2018-047**
DISCLOSURE OF CERTIFICATE OF LIVE BIRTH

200 **Advisory Opinion No. 2018-049**
DISCLOSURE OF PERSONAL INFORMATION TO THE POLICE AND THE MEDIA

207 **Advisory Opinion No. 2018-050**
COLD CALLS AND EMAILS

213 **Advisory Opinion No. 2018-051**
VARIOUS CONCERNS REGARDING THE DATA PRIVACY ACT

222 **Advisory Opinion No. 2018-052**
CHED MEMORANDUM ORDER NO. 3, SERIES OF 2012

226 **Advisory Opinion No. 2018-053**
PHOTOGRAPHS AND CCTV FOOTAGES IN HOSPITALS

230 **Advisory Opinion No. 2018-054**
PATIENT REGISTRY, RESEARCH, AND THE DATA PRIVACY ACT OF 2012

234 **Advisory Opinion No. 2018-056**
WEB-BASED ACCREDITATION SYSTEM FOR HOSPITALS

238 **Advisory Opinion No. 2018-057**
OUTSOURCING AGREEMENT

242 **Advisory Opinion No. 2018-058**
AYALA REWARDS CIRCLE

249 **Advisory Opinion No. 2018-059**
SKIP TRACING AND PROBING OF CONTACT DETAILS THROUGH THE INTERNET AND THIRD PARTIES

254 **Advisory Opinion No. 2018-060**
DISCLOSURE OF PERSONAL INFORMATION TO THE BANGKO SENTRAL NG PILIPINAS

258 **Advisory Opinion No. 2018-061**
PROCESSING OF PERSONAL INFORMATION FOR CHARACTER REFERENCE

262 **Advisory Opinion No. 2018-062**
DISCLOSURE OF PERSONAL DATA OF PATENT AND TRADEMARK APPLICANTS AND INVENTORS

266 **Advisory Opinion No. 2018-063**
REVIEW OF CONSENT FORM

271 **Advisory Opinion No. 2018-064**
CLARIFICATIONS ON ISSUANCE OF PRESS RELEASES BY THE PHILIPPINE DEPOSIT INSURANCE CORPORATION

274 **Advisory Opinion No. 2018-066**
SUBMISSION OF REQUIRED PERSONAL DATA OF PATIENTS WHO UNDERGO DRUG TESTING TO THE DEPARTMENT OF HEALTH

278 **Advisory Opinion No. 2018-067**
OWWA E-CARD PROJECT

282 **Advisory Opinion No. 2018-069**
PHONE USAGE DATA RECORDS

285 **Advisory Opinion No. 2018-070**
MUNTINLUPA CITY ORDINANCE NO. 96-80

288 **Advisory Opinion No. 2018-071**
DISCLOSURE OF SCHOOL RECORDS FOR INVESTIGATION PURPOSES

292 **Advisory Opinion No. 2018-072**
REVIEW OF CONSENT FORM

297 **Advisory Opinion No. 2018-076**
SUBMISSION OF PERSONAL DATA OF SEAFARERS TO THE MARITIME INDUSTRY AUTHORITY

305 **Advisory Opinion No. 2018-077**
CONGRESSIONAL REQUEST FOR LISTS OF BENEFICIARIES OF THE PANTAWID PAMILYANG PILIPINO PROGRAM (4Ps) AND THE SOCIAL PENSION FOR INDIGENT SENIOR CITIZENS PROGRAM

311 **Advisory Opinion No. 2018-078**
DISCLOSURE OF PERSONAL DATA FOR THE DEPARTMENT OF LABOR AND EMPLOYMENT'S AUDIT OF EMPLOYERS

317 **Advisory Opinion No. 2018-080**
VIEWING AND/OR RELEASE OF CCTV FOOTAGES

321 **Advisory Opinion No. 2018-081**
ACCESS TO MEDICAL RECORDS IN CR-DR SYSTEM

325 **Advisory Opinion No. 2018-083**
COLLECTION OF HEALTH INFORMATION BY THE DEPARTMENT OF HEALTH

330 **Advisory Opinion No. 2018-084**
COMPUTER MONITORING

334 **Advisory Opinion No. 2018-088**
DENIAL OF REQUEST FOR DISCLOSURE OF THE PERSONAL DATA SHEET BY THE CITY OF SAN JUAN

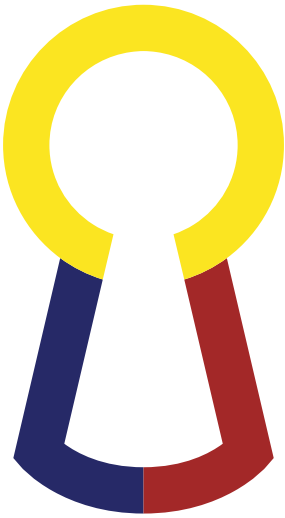
336 **Advisory Opinion No. 2018-090**
DATA PRIVACY AND OFFICE-ISSUED MOBILE DEVICES

343 **NPC CASES & DECISIONS**

344 **NPC Case No. 18-058**
WENDY'S RESTAURANT, INC. (PHILIPPINE REPRESENTATIVE OFFICE) DATA BREACH (2018)

346 **NPC Case No. 17-043**
JOLLIBEE FOODS CORPORATION

349 **NPC Case No. 18-J-162**
FACEBOOK FORCED LOGOUT



NATIONAL
PRIVACY
COMMISSION

5th Floor Delegation Building
Philippine International Convention Center (PICC) Complex
Roxas Boulevard, Manila, 1307

NPC MEMORANDUM CIRCULARS

- **NPC CIRCULAR NO. 18-01**
  Rules of Procedure on Requests for Advisory Opinions
- **NPC CIRCULAR NO. 18-02**
  Guidelines on Compliance Checks
- **NPC CIRCULAR NO. 18-03**
  Rules on Mediation before the National Privacy Commission

NPC CIRCULAR
NO. 18-01

DATE 10 September 2018

Rules of Procedure on Requests for Advisory Opinions

Pursuant to the authority vested in the National Privacy Commission (NPC) through Section 7 of Republic Act No. 10173, otherwise known as "The Data Privacy Act of 2012" (DPA), the following guidelines for requests for advisory opinions of the NPC are hereby prescribed and promulgated:

RULE I
PRELIMINARY PROVISIONS

SECTION 1. General Principles. – The NPC is an independent body mandated by law to provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person. It is authorized to promulgate rules to facilitate the drafting of opinions, determine the requirements, and provide guidelines to ensure efficiency in the administration and adequacy of response to the requesting party.

SECTION 2. Advisory Opinion. – An advisory opinion refers to a determination of the NPC on matters relating to data privacy or data protection, at the request of any party, or on a complaint endorsed by the Complaints and Investigations Division (CID) under Sections 4 and 10 of Rule II of NPC Circular No. 2016-04.

It shall be based only on the facts and circumstances provided by the requesting party, taking into account applicable laws and regulations. It shall serve to provide guidance to the requesting party and the general public, but shall not be used in the nature of a standing rule binding on the NPC when evaluating other cases regardless of the similarity of the facts and circumstances.

An advisory opinion shall neither adjudicate issues between parties nor impose any sanctions or award damages. It may be referred to the CID for evaluation, investigation and appropriate action, as may be necessary.

SECTION 3. Scope and Coverage. – These rules shall apply to all requests for advisory opinions cognizable by the NPC.

RULE II
REQUIREMENTS FOR REQUESTS FOR ADVISORY OPINIONS

SECTION 4. Letter Request. – The requesting party shall submit a letter request for the issuance of an advisory opinion, addressed to the Privacy Commissioner and Chairman. The letter request may be delivered to the NPC personally, or sent by direct or electronic mail.

The following information shall be indicated in the letter request:

a. Name, complete business or postal address, telephone and e-mail address of the requesting party;

b. Novel issues, questions of law or matters and other legitimate concerns sought to be clarified or confirmed by the requesting party;

c. A comprehensive narrative of the factual circumstances and legal bases of the request;

d. An affidavit or certification that the subject of the request for advisory opinion is not a matter pending in a case in litigation before the courts, the NPC or is not subject of an ongoing investigation or compliance check; and

e. All relevant documents and attachments that will enable the NPC to appropriately respond to the request.

The letter request shall not be required if the matter is endorsed by the CID under Rule II of NPC Circular No. 2016-04.

SECTION 5. Subject of an advisory opinion. A PIC or PIP in the government or private sector may be subject to a Compliance Check based on any of the following considerations:

a. The following may be the subject of an advisory opinion:

    1. Interpretation of the provisions of the DPA, its Implementing

[1] Affidavit duly notarized for individual data subjects and Secretary's Certificate for juridical persons. This documentary requirement may be waived in meritorious cases.z

Rules and Regulations (IRR) and NPC Issuances;

2. Compliance requirements under the DPA and related issuances;

3. Enforcement of data privacy laws and regulations; and

4. Other related matters on personal data privacy, security, and protection.

b. A request for advisory opinion shall not be accommodated if:

1. The request is on an issue which has been finally decided by the courts or is pending in a case in litigation;

2. The request is related to any matter before the NPC, or is subject of an ongoing investigation or compliance check;

3. The request has previously been the subject of an advisory opinion;

4. The request posits questions, issues or concerns that are too general in scope, overly abstract, anticipatory and speculative;

5. The request requires a review and interpretation of contracts or an opinion on the validity of contracts; or

6. It involves a request for review of a privacy notice, privacy manual, consent form, organization terms and conditions, or other privacy policies.

7.

If the request for advisory opinion shall be denied for any of the reasons mentioned above, the NPC shall send a notice of denial of request. The requesting party may decide to complete the documentary requirements, if such is the basis for denial and re-file the request.

Requests with inordinate number of questions are also discouraged to allow for the expeditious resolution of all pending requests. The NPC reserves the right to evaluate each request and resolve the same in a manner it deems fit.

SECTION 6. Supporting documents. – The requesting party must submit all pertinent documents and provide all information for the evaluation of the request. The NPC may request for additional information as may be necessary to evaluate the request or to effectively respond to the inquiry presented.

SECTION 7. Withdrawal of a request. – The requesting party may file a letter of withdrawal to formally withdraw the request for an advisory opinion in the event the matter becomes moot and academic, the issue inquired upon has been resolved in another advisory opinion which has been published by the NPC, or for any other valid reason, at any time before the NPC issues and transmits the advisory opinion to the requesting party; Provided, that the NPC may proceed to render said opinion at its discretion.

SECTION 8. Filing as a complaint. – If during the pendency of the request for advisory opinion, the requesting party decides to file the matter as a complaint cognizable by the CID, the request for advisory opinion previously filed shall be held in abeyance.

The complaint shall be handled in accordance with NPC Circular 16-04. All documents attached, as stated in the request for advisory opinion, and the findings during the proceedings thereof, shall not be adopted by the CID in its investigation, unless such documents have been formally offered by the parties as evidence.

The complaint shall be given precedence over the request for advisory opinion as the complaint will involve the adjudication of issues, determination of rights of the parties and imposition of sanctions. If the complaint is dismissed, or otherwise terminated, the request for advisory opinion shall proceed accordingly.

SECTION 9. Conference with the Requesting Party. – Where necessary, the NPC may, in its discretion, require the requesting party to attend a conference, for a more exhaustive and thorough discussion of the matter.

RULE III
GENERAL PROVISIONS

SECTION 10. Release of Advisory Opinions. – The advisory opinion shall be released to the requesting party not later than twenty (20) working days from date of receipt by the concerned division, unless the complexity and novelty of the subject matter requires a longer period of time for further evaluation. The requesting party shall be notified of the reason for the extension.

A scanned copy of the document shall be sent electronically, or the hard copy shall be mailed to the business address provided by the requesting party.

SECTION 11. Publication of Advisory Opinions. – Advisory opinions issued by the NPC shall be made available to the public through publication by print or on the official website of the NPC. However, all sensitive personal information and/or critical business or proprietary information shall be kept confidential. Such details shall be redacted or anonymized in the published version.

SECTION 12. Fees. – Every request for the issuance of an advisory opinion may be subject to a reasonable fee, as may be prescribed by the NPC in a separate issuance.

SECTION 13. Separability Clause. – If any portion or provision of these Rules is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 14. Repealing Clause. – All other rules, regulations, and issuances contrary to or inconsistent with the provisions of these Rules are deemed repealed or modified accordingly.

SECTION 15. 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 E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Date: **10 September 2018**

NPC CIRCULAR
NO. 18-02

DATE 20 September 2018

Guidelines on Compliance Checks

WHEREAS, The right to privacy, which includes information privacy, is constitutionally protected and accorded recognition independent of its identification with liberty, and at the same time, Article II, Section 11 of the Constitution values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Article II, Section 24, of the Constitution provides that the State recognizes the vital role of communication and information in nation-building, and Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;

WHEREAS, Section 7 of the DPA provides that the National Privacy Commission (Commission) shall administer and implement the provisions of the DPA, monitor and ensure compliance of the country with international standards set for data protection, and ensure compliance of Personal Information Controllers with the provisions of the DPA, and Section 14 of the DPA also requires Personal Information Processors to comply with all the requirements of the Act and other applicable laws;

WHEREAS, Section 7 of the DPA provides that the Commission can compel any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy, or coordinate with government and the private sector in implementing plans and policies to strengthen personal data protection;

WHEREAS, in order to ensure compliance of the country and all PICs and PIPs with the law and international standards set for data protection, including adherence to data privacy principles, implementation of security measures, and provisions for data subjects to exercise their rights, Section 29 of the Implementing Rules and Regulations (IRR) provides that the Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures.

WHEREFORE, in consideration of these premises, the Commission hereby issues this Circular governing the conduct of Compliance Checks.

I. GENERAL PROVISIONS

SECTION 1. Scope. These Rules shall apply to any Personal Information Controller (PIC) or Personal Information Processor (PIP) in the government or private sector processing personal data in the Philippines, subject to the relevant provisions of the Act and its Implementing Rules and Regulations.

SECTION 2. Purpose. These Rules provide the guidelines for the conduct of Compliance Checks by personnel of the Commission, whichever mode it may be. Compliance Checks are undertaken for the following purposes:

A. Protect individuals and their personal data by cultivating a culture of privacy in all agencies, companies and organizations involved in the processing of personal data;

B. Effectively administer and implement the DPA by strengthening the regulatory environment in the country and the Commission's ability to identify and take action on non-compliance, with the interest and welfare of the people as a primary consideration; and,

C. To emphasize the importance of accountability, to the end that PICs and PIPs are allowed the opportunity to demonstrate compliance with the DPA, its IRR and relevant rules and regulations, and to promote the building of trust between data subjects and those involved in the processing of personal data, whether the government or the private sector.

SECTION 3. 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, otherwise known as the Data Privacy Act of 2012;

B. "Certificate of No Significant Findings" refers to an issuance of the Commission to a Personal Information Controller or Personal Information Processor which serves as a certification that it has undergone a Compliance Check and there were no notable findings requiring further action from the Commission.

The Certificate also refers to an issuance which certifies that an entity has undergone a Compliance Check with findings of substantial deficiencies, and has implemented remediation measures as ordered by the Commission.

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

D. "Compliance Check" refers to the systematic and impartial evaluation of a PIC or PIP, in whole or any part, process or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the Data Privacy Act and other issuances of the Commission. It is an examination, which includes Privacy Sweeps, Documents Submissions and On-Site Visits, intended to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls and review mechanisms intended to assure privacy and personal data protection in data processing systems.

E. "Compliance Order" refers to an issuance of the Commission to a PIC or PIP directing it to perform actions, institute measures or any other prescriptions of the Commission in relation to the Compliance Check conducted.

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;

G. "Data Protection Officer" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission.

H. "Document Submission" refers to a mode of Compliance Check as defined under Section 4 (B) of this Circular.

I. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012.

J. "Notice of Deficiencies" refers to a document issued by the Commission indicating the deficiencies of a PIC or PIP found to be non-compliant upon the conduct of a Compliance Check, taking into consideration the provisions of the DPA, its IRR, and the relevant issuances and orders of the NPC.

K. "On-Site Visit" refers to a mode of Compliance Check as defined under Section 4 (C) of this Circular.

L. "Personal Data" refers to all types of personal information, and sensitive personal information as defined under R.A. No. 10173.

M. "Personal Information Controller" (PIC) refers to a natural or

juridical person, or any other body that controls the processing of personal data, or instructs another to process personal data on its behalf.

N. "Personal Information Processor" (PIP)(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 pertaining to a data subject.

O. "Privacy Compliance Questionnaire" is a document containing a series of questions formulated by the Commission to be answered by the PIC or PIP to contextualize documents and policies that the Commission requires to be submitted.

P. "Privacy Sweep" refers to a mode of Compliance Check as defined under Section 4 (A) of this Circular.

II. GUIDELINES FOR THE CONDUCT OF COMPLIANCE CHECK

SECTION 4. Modes of Compliance Checks. In ensuring compliance with the Act and its related issuances, the Commission may employ any of the following modes of Compliance Checks:

A. Privacy Sweep. The Commission shall review a PICs or PIPs compliance with respect to its obligation under the DPA, and its related issuances based on publicly available or accessible information, such as, but not limited to, websites, mobile applications, raffle coupons, brochures, and privacy notices. This is the initial mode of Compliance Check.

B. Documents Submission. The Commission may require the submission of documents and additional information from a PIC or PIP that has undergone a privacy sweep to, among others, clarify certain findings arising therefrom, and to determine the level of compliance of the PIC or PIP with respect to its obligations under the DPA and its related issuances.

C. On-Site Visit. The Commission may subject a PIC or PIP to an on-site visit if there are persistent or substantial findings of non-compliance with the obligations indicated in the DPA and its related issuances.

Authorized personnel of the Commission shall conduct a targeted inspection within the premises of a PIC or PIP that may include a presentation of documents or records, visits to selected departments

wherein processing of personal information are undertaken, as well as interviews of relevant personnel tasked to handle personal information processed by the PIC or PIP subject to the Compliance Check.

Authorized personnel of the Commission shall conduct a targeted inspection within the premises of a PIC or PIP that may include a presentation of documents or records, visits to selected departments wherein processing of personal information are undertaken, as well as interviews of relevant personnel tasked to handle personal information processed by the PIC or PIP subject to the Compliance Check.

The Commission may, in its discretion, directly employ this mode of Compliance Check if it determines that the totality of circumstances warrant such action, taking into account the next succeeding provision.

SECTION 5. Considerations for the Conduct of Compliance Checks. A PIC or PIP in the government or private sector may be subject to a Compliance Check based on any of the following considerations:

a) Level of risk to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;

b) Reports received by the Commission against the PIC or PIP, or its sector;

c) Non-registration of a PIC or PIP that is subject to the mandatory registration requirement as provided under NPC Circular 17-01;

d) Unsecured or publicly available personal data found on the internet that may be traced to a PIC or PIP; and

e) Other considerations that indicate non-compliance with the DPA or the issuances of the Commission.

In cases where the Complaints and Investigations Division (CID) of the Commission is investigating or commences an investigation against a PIC or PIP undergoing or scheduled for Compliance Check, the Compliance Check shall be held in abeyance and the investigation shall be given precedence.

SECTION 6. When to Conduct Compliance Check. An On-Site Visit may be conducted during regular office hours except Saturdays, Sundays and legal holidays. Privacy Sweep, Documents Submission, or investigations conducted by the CID are not subject to such limitations; Provided, if the last day of the period to comply with an order for Document Submission, falls on a Saturday a Sunday, or a legal holiday, the last day shall be the next working day.

SECTION 7. Notice of Compliance Checks. The Commission shall send a Notice, accompanied with a Privacy Compliance Questionnaire, to a PIC or PIP regarding the conduct of a Compliance Check through the electronic mail (e-mail) address used at the time they registered with the Commission. Such Notice shall be deemed received on the next business day; Provided, for unregistered organizations, the Notice shall be sent to their registered business address via courier addressed to the head of the organization.

A PIC or PIP shall take the necessary steps to ensure that their registered e-mail address is working and able to receive the Notice promptly.

A Notice of Compliance Check will be sent in the following instances:

a) Documents Submission. The Commission shall send a Notice to the PIC or PIP requiring the submission of specific documents or policies in a machine-readable or other commonly used file format, within a given period of time, which shall not be less thanz ten (10) days. This period stated in the Notice will be determined based on the nature of the findings in the Privacy Sweep.

b) On-site Visit. The Commission shall send a Notice to the PIC or PIP at least ten (10) days before such visit. The Notice shall include an Order for the Presentation of Documents or Records, Conduct of Interviews, Inspection of Premises and Equipment and other necessary activities.

The on-site visit team shall bring an Order from the Commission identifying those authorized to conduct the inspection, and shall display proper identification tags issued by the Commission.

SECTION 8. Issuance of Notice of Deficiencies. If the PIC or PIP is found to be non-compliant with the DPA, its IRR, and other issuances of the Commission, the Commission shall issue a Notice of Deficiencies indicating the period of time within which to correct the identified deficiencies, which shall not be less than ten (10) days. The DPO, or in the case of unregistered entities, the head of the organization, shall file with the Commission a report on the actions taken.

SECTION 9. Issuance of Compliance Order. The Commission shall issue a Compliance Order in the following instances:

a) After the lapse of the period provided in the Notice of Deficiencies and no action was taken by the PIC or PIP to

correct the identified deficiencies.

b) After the lapse of the period provided in the Notice of Deficiencies and such identified deficiencies persist.

c) If the persistence of the deficiencies is due to the considerable period of time or resources needed to implement the necessary remediation measures, the timeline to complete such measures, as approved by the Comission, shall be embodied in a Compliance Order.

d) In the course of the conduct of an on-site visit, the PIC or PIP refuses or fails to provide access to premises, records or prevents the conduct of the inspection.

Compliance Orders shall state the deficiencies remaining or actions to be taken, the period within which to undertake the corrections ordered by the Commission, and the period to report such actions.

SECTION 10. Issuance of Other Orders. The Commission may issue any and all pertinent orders in connection with the conduct or furtherance of a Compliance Check or the assessment of any organization's compliance with any orders in relation thereto.

SECTION 11. Certificate of No Significant Findings. The Commission shall issue a Certificate of No Significant Findings to a PIC or PIP that has undergone Document Submission or an On-site Visit, where no substantial deficiencies were found or the deficiencies identified in the Notice of Deficiencies have already been addressed to the satisfaction of the Commission.

The issuance of this Certificate is without prejudice to any other recommendation being made by the Commission for the improvement of the organization's compliance with the DPA and related issuances. The issuance of this Certificate does not bar an investigation for any possible liability arising from complaints and/or personal data breaches filed before the Commission.

SECTION 12. Failure to Comply with Compliance Order. Deficiencies that are not corrected by the PIC or PIP within the prescribed period stated in the Compliance Order may subject the PIC or PIP to criminal, civil or administrative penalties, without prejudice to other remedies available under the law.

SECTION 13. Refusal to Undergo Compliance Check. A PIC or PIP who, without good reason and despite due notice, refuses or prevents the Commission from performing a Compliance Check may be subject to appropriate sanctions as may be allowed by law. In case of refusal, the following provisions shall govern:

A. Action to be Taken upon Refusal or Failure to Comply with Documents Submission and Complete the Privacy Compliance Questionnaire. Refusal or failure to submit the requested documents or policies, or submit a completed Privacy Compliance Questionnaire, within the period stated in the Notice or Order, shall subject a PIC or PIP to an on-site visit from the Commission, enforcement actions, and such other fines and penalties as may be appropriate under the circumstances.

B. Action to be Taken upon Refusal or Failure to Provide Access to Premises or Records during an On-site Visit. Refusal or failure to provide access to premises or records during an on-site visit shall subject a PIC or PIP to a Compliance Order, enforcement actions, and such other fines and penalties as may be appropriate under the circumstances

C. Failure or Refusal to Provide an Explanation to Compliance Orders. Refusal or failure to submit an explanation to the Order cited in the preceding paragraphs, or if the explanation does not present a compelling reason to justify such refusal or failure, may subject a PIC or PIP to contempt

SECTION 14. Fines and Penalties. Failure to comply with the DPA, other issuances, or orders of the Commission may subject a PIC or PIP to fines and penalties as may hereafter be prescribed by the Commission.

III. MISCELLANEOUS PROVISIONS

SECTION 15. Publication. To protect the public, and in keeping with the Commission's mandate to inform the public on data subject rights, as well as the compliance of PICs and PIPs with their obligations under the law, the results of the Compliance Checks, and orders issued in relation thereto may be published by the Commission at its discretion.

SECTION 16. Separability Clause. If any portion or provision of this Circular is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 17. Effectivity Clause. This Circular shall take effect immediately after publication in the Official Gazette or two (2) newspapers of general circulation.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Date: **20 September 2018**

NPC CIRCULAR
NO. 18-03

DATE 18 December 2018

Rules on Mediation before the National Privacy Commission

Pursuant to the authority vested in the National Privacy Commission through Section 7(b) of Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012," to facilitate or enable settlement of complaints through the use of alternative dispute resolution processes; and consistent with Republic Act No. 9285, otherwise known as the "Alternative Dispute Resolution Act of 2004," declaring it the policy of the State to actively promote party autonomy in the resolution of disputes and the freedom of the parties to make their own arrangements to resolve their disputes, the following Rules on Mediation before the National Privacy Commission are hereby prescribed and promulgated.

RULE I
PRELIMINARY PROVISIONS

SECTION 1. Application and Interpretation. In applying and construing the provisions of these Rules, consideration must be given to the need to promote candor among the parties, the confidentiality of the mediation process, and the independence of the determination and resolution of the parties of their dispute, all of which shall foster prompt, economical, and amicable resolution of disputes.

SECTION 2. Scope. These Rules shall apply to all complaints filed before the Commission.

SECTION 3. Definition of Terms. For the purpose of this Circular, the following terms are defined, as follows:

a. Commission – refers to the National Privacy Commission.

b. Complaint Proceedings – proceedings before the Complaints and Investigation Division commenced sua sponte or by the filing of a sworn affidavit or verified complaint, including investigations, except those arising from breach notifications.

c. Discovery Conference – a meeting pursuant to an Order to Confer for Discovery issued by the investigating officer during complaint proceedings.

d. Investigating Officer – refers to the personnel of the Complaints and Investigation Division assigned by the Commission to preside over complaint proceedings.

e. Mediation – refers to the voluntary process in which a mediation officer facilitates communication and negotiation, and assists the parties in reaching a voluntary agreement regarding a dispute.

f. Mediation Officer – refers to the personnel of the Legal Division assigned or designated by the Commission to conduct mediation.

RULE II
PROCEDURE

Section 1. Willingness to Mediate. – The parties, by mutual agreement, may signify their interest to explore the possibility of settling the dispute by mediation during the discovery conference or at any stage of the complaint proceedings thereafter.

Section 2. Application for Mediation. – The parties shall jointly file with the investigating officer an Application for Mediation manifesting their earnest commitment to engage in a meaningful settlement process and their willingness to abide by these Rules and the orders issued by the assigned mediation officer. No application for mediation shall be approved without payment of the mediation fee.

Section 3. Order to Mediate. – The investigating officer shall issue an Order to Mediate, which shall state the following: (a) the approval of the Application for Mediation; (b) the suspension of the complaint proceedings for sixty (60) days pending the mediation proceedings; (c) the name of the assigned or designated mediation officer who shall preside over the mediation proceedings; and (d) the date, time, and place when the parties shall appear before the mediation officer for the preliminary mediation conference. Copies of the Order to Mediate shall be furnished to the mediation officer and the parties.

Section 4. Preliminary Mediation Conference. – The mediation officer shall receive the appearances of the parties and inform them of the mediation process and the manner by which the proceedings will be conducted. The mediation officer shall stress the benefits of an early settlement of the dispute and endeavor to achieve the most fair and expeditious settlement possible.

Each party shall be allowed to make a brief statement of their respective position and preferred outcome. The mediation officer shall explore common ground for settlement and suggest options for the parties to consider.

When necessary, the parties shall agree on the schedule of the next mediation conference and the mediation officer shall issue an order therefor.

Section 5. Separate Caucuses and Subsequent Conferences. – The mediation officer may, with the consent of both parties, hold separate caucuses with each party to enable a determination of their respective real interest in the dispute; provided, that each party shall be afforded equal time and/or opportunity to ventilate such interest and motivation. The mediation officer may call such conferences/caucuses as may be necessary to facilitate settlement.

The mediation officer shall hold in confidence any matter disclosed during the separate caucuses and shall exercise reasonable prudence and discretion in the safeguarding of such information.

Section 6. Mediation Period and Extension thereof. – The mediation officer shall endeavor to achieve a mediated settlement of the dispute within fifteen (15) days from the preliminary mediation conference, but shall, in every case, be afforded the initial period of sixty (60) days to achieve the same.

Upon reasonable ground to believe that settlement may yet be achieved beyond the initial mediation period of sixty (60) days, the period to mediate may be extended for another thirty (30) days by the mediation officer. Should no agreement be reached within the extended period, another non-extendible period of thirty (30) days may be jointly requested by the parties subject to the discretion of the mediation officer.

Section 7. Mediated Settlement Agreement. – A mediated settlement agreement following successful mediation shall be jointly prepared and executed by the parties, with the assistance of their respective counsel, if any. The execution of a mediated settlement agreement shall terminate the mediation proceedings. The mediation officer shall certify that the contents of the agreement have been explained, understood, and mutually agreed upon by the parties, and that the provisions thereof are not contrary to law, public policy, morals, or good customs.

Section 8. Confirmation by the Commission. – The mediation officer shall issue a resolution submitting the mediated settlement agreement to the Commission within five (5) days from the signing and filing thereof. Copies of the resolution shall be furnished to the parties and the investigating officer. The Commission shall thereafter issue a resolution

confirming the mediated settlement agreement within fifteen (15) days from submission of the resolution and mediated settlement agreement.

Section 9. Effect of Confirmed Mediated Settlement Agreement. – A confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint, and shall be enforced in accordance with the Commission's rules and issuances.

Section 10. Failure to Reach Settlement. – If the parties are unable to arrive at a settlement of their dispute, or it becomes apparent that a settlement, given the disparity of the respective positions of the parties, is not likely or achievable within the sixty (60) day mediation period or the reasonable extension of such period under Section 7, the mediation officer may declare the mediation unsuccessful and terminate the proceedings by issuing a Notice of Non-Settlement of Dispute and furnishing the investigating officer and the parties with copies thereof.

Section 11. Resumption of Complaint Proceedings. – Upon receipt of the Notice of Non- Settlement of Dispute issued by the mediation officer, the investigating officer shall issue an order lifting the suspension of the complaint proceedings, which shall resume as a matter of course. Copies of the order, including the notice of the next hearing date of the complaint proceedings, shall be furnished to all the parties.

Section 12. Field Mediation. – The personnel of the Legal Division shall be authorized to conduct mediation proceedings between parties during the conduct of regional discovery conferences by the Complaints and Investigation Division.

RULE III
GENERAL PROVISIONS

Section 1. Personal Appearance by the Parties. – Individual parties are required to personally appear during mediation conferences. Representatives may appear on behalf of individual parties; provided, that they are authorized by special power of attorney to appear, offer, negotiate, accept, decide, and enter into a mediated settlement agreement without additional consent or authority from the principal. If the party is a partnership, association, corporation, or a government agency, the representative must be authorized by a notarized Secretary's Certificate, Board Resolution, or any equivalent written authority to offer, negotiate, accept, decide, and enter into a mediated settlement agreement.

Section 2. Effect of Failure of Parties to Appear. – If any of the parties fail to appear without prior notice and justifiable reason for two (2) consecutive mediation conferences/caucuses at any stage of the mediation, the mediation officer may order the termination of the mediation proceedings. The mediation officer may also require the non-appearing party to explain why said party should not be required to pay treble the costs incurred by the appearing party, including attorneys fees, in attending the mediation conferences/caucuses, and be henceforth permanently prohibited from requesting mediation at any other stage of the complaint proceedings before the Commission.

Section 3. Presence of Lawyers in Mediation. – Lawyers, upon the discretion of the mediation officer, may attend the mediation conferences in the role of adviser and consultant to their clients and shall cooperate with the mediation officer towards securing a settlement of the dispute. They shall help their clients comprehend the mediation process and its benefits and assist in the preparation of a mediated settlement agreement and its eventual enforcement.

Section 4. Venue. – Mediation proceedings shall be conducted within the Commission premises. Upon request of both parties, the mediation officer may authorize the conduct of a mediation conference at any other venue, provided that all related expenses, including transportation, food, and accommodation, shall be borne by both parties. If a change of venue is requested by one party, it must be with the other's conformity and they shall agree on the terms of handling the expenses.

Section 5. Confidentiality. – The mediation conferences shall be held in private. Persons other than the parties, their representatives, counsel, and the mediation officer may attend only with the consent of the parties and upon approval by the mediation officer. Anyone present during a mediation conference shall not disclose any information obtained in the course thereof to any other person, nor utter the same through other means.

The mediation proceedings and all incidents thereto shall be kept strictly confidential, and all admissions or statements therein shall be inadmissible for any purpose in any proceeding, unless otherwise specifically provided by law. However, evidence or information that is otherwise admissible or subject to discovery does not become inadmissible or protected from discovery solely by reason of its use in mediation.

No transcript or minutes of the mediation proceedings shall be taken, and the personal notes of the mediation officer, if any, shall likewise be

inadmissible nor cognizable in any court, tribunal, or body for whatever purpose and shall be securely destroyed upon termination of the mediation proceedings.

Section 6. Mediation Fees. – The mediation fee in an amount prescribed by the Commission shall be paid by the parties upon the filing of the Application for Mediation.
Complainants may be exempted from the payment of the mediation fee and enter into mediation proceedings as indigents upon submission of a certificate of indigency issued by the barangay captain at their place of residence.

RULE IV
MISCELLANEOUS PROVISIONS

Section 1. Amendments. – These Rules or any portion thereof may be amended or supplemented by the Commission.

Section 2. Separability Clause. – If any part, article, or provision of these Rules are declared invalid or unconstitutional, the other parts not affected shall remain valid.

Section 3. Transitory Provision. – These Rules shall apply to pending complaints, provided the parties express their interest to settle the dispute by mediation.

Section 4. Effectivity. – These Rules shall take effect fifteen (15) days after publication in a newspaper of general circulation.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Date: **18 December 2018**

ANNEX "A"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s CID Case No.

- versus -

_____
Respondent/s

APPLICATION FOR MEDIATION

The undersigned parties wish to settle matters in dispute between them without resorting to the adversarial process. The parties and their counsel, if any, manifest their earnest commitment to engage in a meaningful settlement process pursuant to the following undertaking:

1. The parties agree that they are entering into the mediation process in good faith and shall make a sincere effort to arrive at a mutually acceptable resolution of the dispute.
2. The parties agree they will rely solely on their own judgment in arriving at a resolution of their dispute.
3. The parties understand that the complaint proceedings before the investigating officer shall be suspended during the pendency of the mediation proceedings before the mediation officer.
4. The parties agree to abide by the Rules on Mediation Before the National Privacy Commission, a copy of which has been furnished the parties, and the orders issued by the assigned mediation officer.

The parties have signed and submitted this Application for Mediation on _____.

Complainant/s	**Respondent/s**
_____	_____
Signature over printed name	*Signature over printed name*
_____	_____
Signature over printed name	*Signature over printed name*
_____	_____
Signature over printed name	*Signature over printed name*

The parties have paid the mediation fee in the amount of ₱_____ as evidenced by Official Receipt No. _____ dated _____, which is attached hereto.

_____
Signature over printed name
Investigating Officer

6

ANNEX "B"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s CID Case No.

\- versus -

_____
Respondent/s

ORDER TO MEDIATE

Finding that the parties have paid the mediation fee as evidenced by Official Receipt No. _____ dated _____, the undersigned investigating officer approves the Application for Mediation filed on _____.

The complaint proceedings are suspended for sixty (60) days starting today for the conduct of the mediation proceedings.

The parties are ordered to appear at the preliminary mediation conference before Atty./Mr./Ms. _____, the mediation officer who shall preside over the mediation proceedings, on (date) _____ at (time) _____ at the office of the National Privacy Commission, 5th floor PICC Delegation Building, CCP Complex, Pasay City.

SO ORDERED.

City of Pasay, (date) _____.

_____
Signature over printed name
Investigating Officer

_____
LD ADR Case No.

_____
Signature over printed name
Mediation Officer

ANNEX "C"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s LD ADR Case No.

\- versus -

_____
Respondent/s

ORDER

At today's preliminary mediation conference/mediation conference

____ the parties were present and agreed to schedule another mediation conference.

____ the complainant/s failed to appear with/without justifiable reason.

____ the respondent/s failed to appear with/without justifiable reason.

The parties are ordered to appear at the next mediation conference on (date) _____ at (time) _____ at the (place) _____.

SO ORDERED.

City of Pasay, (date) _____.

_____
Signature over printed name
Mediation Officer

ANNEX "D"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s LD ADR Case No.

\- versus -

_____
Respondent/s

MEDIATED SETTLEMENT AGREEMENT

This MEDIATED SETTLEMENT AGREEMENT is entered into between the complainant/s and the respondent/s, collectively referred to as the "parties."

WHEREAS, the parties filed their Application for Mediation on _____ and the preliminary mediation conference was conducted on _____ with the undersigned as mediation officer;

WHEREAS, the parties were able to arrive at an amicable resolution of their dispute, and now wish to commit the terms of their accord into this Mediated Settlement Agreement;

NOW THEREFORE, the foregoing considered, the parties agree as follows:

1. The terms of this Mediated Settlement Agreement shall be enforced in accordance with the Commission's rules and issuances.

2. The parties agree that all information and documents attached to this Mediated Settlement Agreement are strictly confidential.

3. In full settlement of the dispute, the respondent/s agree/s to pay the complainant/s the amount of (words) _____ (figures) ₱_____.

4. Furthermore, respondent/s undertake/s to _____
_____
_____
_____.

5. On the other hand, complainant/s commit/s to _____
_____
_____
_____.

6. In consideration of their faithful performance of the terms of this Mediated Settlement Agreement, the parties, for themselves, their successors, and assigns, do hereby relinquish, waive, release, acquit, and forever discharge each other of and from any and all claims, disputes, complaints, causes of action, and rights

based on actions or events which occurred prior to the date of this Mediated Settlement Agreement.

7. A party's rights under this Mediated Settlement Agreement may not be assigned without the express written consent of the other party.

8. This Mediated Settlement Agreement constitutes the entire agreement between the parties concerning the foregoing settlement and release of claims.

IN WITNESS WHEREOF, the parties have executed this Mediated Settlement Agreement this ____ day of _____, 20___.

Complainant/s	**Respondent/s**
_____	_____
Signature over printed name	*Signature over printed name*
_____	_____
Signature over printed name	*Signature over printed name*
_____	_____
Signature over printed name	*Signature over printed name*

ANNEX "E"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s LD ADR Case No.

\- versus -

_____
Respondent/s

RESOLUTION

WHEREAS, on (date) _____, the instant complaint was filed based on the following facts: (Provide a brief statement of the facts.)

_____
_____
_____
_____
_____
_____;

WHEREAS, the parties filed their Application for Mediation on _____ and the preliminary mediation conference was conducted on _____ with the undersigned as mediation officer;

WHEREAS, through the sincere effort of the parties to arrive at an amicable resolution of their dispute, they were able to execute a mediated settlement agreement;

WHEREAS, the mediation proceedings has been terminated through the execution of the mediated settlement agreement;

WHEREAS, a confirmed mediated settlement agreement shall have the effect of a decision or judgment on the complaint and shall be enforced in accordance with the Commission's rules and issuances.

WHEREFORE, in view of the foregoing, the undersigned mediation officer submits the attached mediated settlement agreement executed by the parties for confirmation by the Commission.

City of Pasay, (date) _____.

_____
Signature over printed name
Mediation Officer

11

ANNEX "F"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s LD ADR Case No.

- versus -

_____
Respondent/s

NOTICE OF NON-SETTLEMENT OF DISPUTE

The mediation proceedings are ordered terminated effective today for the following reason/s:

____ The parties are unable to reach a settlement.
____ Failure of complainant/s to appear without prior notice and justifiable reason for two (2) consecutive mediation conferences/caucuses.
____ Failure of respondent/s to appear without prior notice and justifiable reason for two (2) consecutive mediation conferences/caucuses.

SO ORDERED.

City of Pasay, (date) _____.

_____
Signature over printed name
Mediation Officer

ANNEX "G"

Republic of the Philippines
NATIONAL PRIVACY COMMISSION

_____ _____
Complainant/s CID Case No.

\- versus -

_____
Respondent/s

ORDER FOR RESUMPTION OF COMPLAINT PROCEEDINGS

On (date) _____, Atty./Mr./Ms. _____, as mediation officer, issued a Notice of Non-Settlement of Dispute between the parties in this case. The Notice of Non-Settlement of Dispute was received by the undersigned on _____.

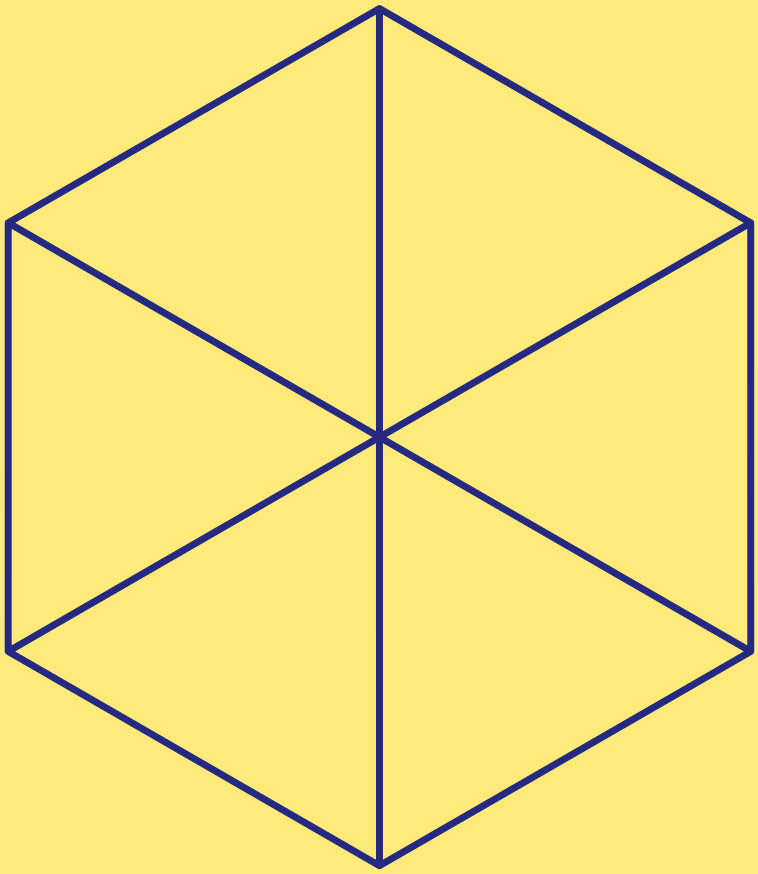
Thus, the suspension of the complaint proceedings is ordered lifted effective today.

The parties are ordered to appear before the undersigned investigating officer for resumption of the complaint proceedings on (date) _____ at (time) _____ at the office of the National Privacy Commission, 5th floor PICC Delegation Building, CCP Complex, Pasay City.

SO ORDERED.

City of Pasay, (date) _____.

_____
Signature over printed name
Investigating Officer



NPC ADVISORIES

NPC CIRCULAR NO. 18-02
Updated Templates on Security Incident and
Personal Data Breach Reportorial Requirements

NPC ADVISORY
NO. 18-02

DATE 26 June 2018

Updated Templates on Security Incident and Personal Data Breach Reportorial Requirements

SEC. 1. Scope. - This Advisory shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the Data Privacy Act of 2012, its implementing rules and regulations, and other relevant issuances of the National Privacy Commission (NPC).

SEC. 2. Updated Templates. - This Advisory provides updated templates for the reportorial requirements of the NPC on security incidents and personal data breaches:

1. Annual security incident reports to be submitted to the NPC by the PIC1 and PIP,2 Provided, that entities that are both PICs and PIPs shall submit both reports to the NPC (both Annex "A" and Annex "B"); and

2. Mandatory notification for the NPC3 and for data subjects4 for personal data breach events with mandatory notification requirements under the Data Privacy Act of 2012.

SEC. 3. The templates pertaining to the Annual Security Incident Reports and Mandatory Breach Notification may be updated in subsequent issuances.

SEC. 4. Online Filing. – Those wishing to submit through the internet may fill out the form at the NPC website; submission through this electronic Form shall be considered as sufficient compliance with the required Annual Security Incident Report. An annual report is not necessary for those who do not experience any security incident within a calendar year.

SEC. 5. This Advisory. – This advisory supersedes and takes precedence over any other prior advisories and issuances inconsistent therewith.

[1] Annex "A" –Annual Security Incident Reports for PICs
[2] Annex "B" –Annual Security Incident Reports for PIPs
[3] Annex "C" – Mandatory Notification: Personal Data Breach for National Privacy Commission
[4] Annex "D" – Mandatory Notification: Personal Data Breach for Data Subjects

Approved:

(sgd.) IVY D. PATDU
Deputy Privacy Commissioner
Policies and Planning

(sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner
Data Processing Systems

(sgd.) RAYMUND E. LIBORO
Privacy Commissioner

ANNEX A

Annual Security Incident Reports for PICs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____City/Municipality: _____ Province: _____

PIC (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION CONTROLLER

A. Personal Data Breach, Mandatory Notification	<#>
B. Personal Data Breach, not covered by mandatory notification requirements	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occurred

Types	***Number***	**Types**	***Number***
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

Personal Data Breaches

	Confidentiality	**Integrity**	**Availability**
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO .: _____

DATE : _____

ANNEX B

Annual Security Incident Reports for PIPs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____City/Municipality: _____ Province: _____

PIP (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION PROCESSOR

This form applies to personal data processing performed on behalf of PICs

A. Personal Data Breaches, reported to PICs	<#>
B. Personal Data Breaches, not reported to PICs	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occurred

Types	***Number***	**Types**	***Number***
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO.: _____

DATE : _____

ANNEX C

Mandatory Notification: Personal Data Breach for the National Privacy Commission

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<PRIVACY COMMISSIONER>
National Privacy Commission
Pasay City, Metro Manila
Philippines

Subject: <DATA BREACH> dated <DATE> of <DATABASE>
<NPC REGISTRATION NO.>

Gentlemen:

I write in behalf of <ENTITY>, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of <ENTITY>, and the responsible persons thereof, are as follows:

Head of the Organization	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Data Protection Officer	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Process Owner	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- *Describe the nature of the personal data breach.*
  - *Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.*

- *Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.*
- *Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.*
- *Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.*
- *Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.*
- *Describe the likely consequences of the personal data breach**. Consider effect on company or agency, data subjects and public.***

Personal Data Possibly Involved.

- *List all sensitive personal information involved, and the form in which they are stored or contained.*
- *Also list all other information involved that may be used to enable identity fraud.*

Measures taken to Address the Breach.

- Describe in full the measures that were taken or proposed to be taken to address the breach.
- Describe how effective these measures are.
- Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.
- Indicate actions of the organization to minimize/mitigate the effect on the affected individual. Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
- Indicate of the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.
- Describe the steps the organization has taken to prevent a recurrence of the incident.

Should you require further information on this matter, contact us using the information above. Any information that later becomes available shall be reported within five (5) days, or as further required by the Commission.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>

ANNEX D

Mandatory Personal Data Breach Notification to Data Subjects

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<DATA SUBJECT>
<ADDRESS>

Subject: <DATA BREACH> dated <DATE>
<NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>.

Nature of the Breach

- *Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.*
- *Describe the likely consequences of the personal data breach.*

Measures taken to Address the Breach.

- **Provide information on** *measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.*
- *Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.*
- *Describe steps the organization has taken prevent a recurrence of the incident.*

Measures taken to reduce the harm or negative consequences of the breach.

- **Describe** *actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.*

Assistance to be provided to the affected data subjects.

- **Include information on** *any assistance to be given to affected individuals.*

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer <DATA PROTECTION OFFICER>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFORMATION>

We undertake to provide more information to you as soon as they become available.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>

NPC ADVISORY OPINIONS

ADVISORY OPINION
NO. 2018-001

5 January 2018

[redacted]

RE: REQUEST FOR OPINION ON THE APPLICABILITY OF THE DATA PRIVACY ACT OF 2012 ON CONTRACTS

Dear [redacted],

This pertains to your request for advisory opinion received by the National Privacy Commission (NPC) on 20 November 2017, which sought guidance regarding Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), particularly its applicability to contracts you execute in the normal course of operations.

Scope

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in the personal information processing.[1] Under Section 3(g) of the DPA, and Section 3(j) of its Implementing Rules and Regulation (IRR), personal information is defined as follows:

> "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."

In addition, Section 3(l) of the DPA defines sensitive personal information as personal information, to wit:

> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

[1] RA No. 10173, §4

(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 person, 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 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.

In your letter request, you have stated that you are collecting the following information:

1. Name;
2. Civil status;
3. Nationality;
4. Principal address; and
5. Information contained in government-issued identification cards.

Based on the definition above, it is clear that the data that you are collecting are considered as personal information and its processing is covered by the DPA, its IRR and issuances of the NPC.

Some information, particularly, the civil status, nationality and the government-issued identification numbers as may be reflected in the ID cards are considered as sensitive personal information. Note that the lawful processing of personal and sensitive personal information should be based on the criteria provided for under Sections 12 and 13 of the DPA, respectively.

[redacted] as Personal Information Controller

In light of the above provisions, it is imperative to note given the nature of data you collect and process from the contracts being entered into, [redacted], as the personal information controller,[2] is expected to comply with its

[2] RA No. 10173, §3(h), **Personal information controller** refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or an organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: (1) A person or organization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes, or uses personal information in connection with an individual's personal, family or household affairs.

duties and responsibilities under the law, i.e. adherence to the principles of transparency, legitimate purpose and proportionality,[3] implementation of reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure,[4] as well as uphold data subjects' rights.[5]

For further information and additional resources, you may visit our website at https://privacy.gov.ph/.

For your reference.

Very truly yours,

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[3] Id., §11
[4] Id., §20(a)
[5] Implementing Rules and Regulations (IRR) of RA No. 10173, §6(a)

ADVISORY OPINION
NO. 2018-002

15 January 2018

[redacted]

Re: COMMISSION ON AUDIT (COA) REQUEST FOR ACCESS TO BANGKO SENTRAL NG PILIPINAS (BSP) EMPLOYEES' DIRECTORY

Dear [redacted],

This is with regard to your query received by the National Privacy Commission (NPC) on 21 November 2017 on the request of the Commission on Audit (COA) for access to the directory of employees posted in the BSP intranet vis-a vis COA's position that it is exempt from the application of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) in the performance of its constitutionally-mandated auditing functions.

We understand that the BSP employee directory contains the following information:

1. Employee name;
2. Position;
3. Office;
4. Office contact numbers;
5. E-mail address; and
6. Photograph.

Scope

Section 4 of the DPA states that the law is applicable to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, including those personal information controllers and processors, who, although not

found or established in the Philippines, use equipment that are located in the Philippines or who maintain an office, branch or agency in the Philippines.

Section 4(a) and (e) states some of the special cases where the law does not apply, to wit:

> "(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
>
> (1) The fact that the individual is or was an officer or employee of the government institution;
> (2) The title, business address and office telephone number of the individual;
> (3) The classification, salary range and responsibilities of the position held by the individual; and
> (4) The name of the individual on a document prepared by the individual in the course of employment with the government.
>
> xxx xxx xxx
>
> (e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. xxx."

Special Cases

In excluding from its scope these categories of information, it does not similarly exclude personal information controllers or personal information processors. Thus, even if a particular information does not fall within the scope of the DPA, this is not a blanket exemption and neither does this exemption extend to the natural or juridical person involved in the personal data processing.

We reiterate that the exemption is not an exemption on the entity or agency but on the type of information processed. This is interpreted to the effect that there is a presumption that personal data may be lawfully processed by a personal information controller or processor under the special cases provided above, but the processing shall be limited to achieving the specific purpose, function or activity, and that the personal information controller or processor remains to be subject

to the requirements of implementing measures to secure and protect personal data.

For instance, a government agency having a constitutional or statutory mandate to collect and process personal data may do so even without the consent of the data subject. But this is with the concomitant responsibility of ensuring that organizational, physical and technical security measures are in place to protect the personal data it is processing.

The exemption particularly pertains to information on any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual information, and information which is necessary in carrying out the functions of a public authority, in accordance to its law enforcement and regulatory mandate under the Constitution or law creating it.

Being an exception to the rule, it must be established that the information claimed to be outside the scope of the DPA is:

1. About a current or former government employee/officer which relates to his or her position or functions; or
2. Necessary in order to carry out the functions of public authority, and processing of personal data is for the performance of a constitutional or statutory mandate.

Thus, only the information required to be processed pursuant to the said function shall not be covered by the law to the minimum extent necessary, while COA, as an entity, is still covered by the DPA.

This means that the COA, as a personal information controller, is mandated under the DPA to adhere to the data privacy principles of transparency, legitimate purpose and proportionality.

In determining whether the personal data being collected by the COA is necessary to carry out its functions, the personal data would have to be processed pursuant to a legitimate purpose, and in a proportional and transparent manner. COA must also implement appropriate security measures for personal data protection, and ensure that data subjects are able to exercise their rights within the limits provided by law.

Thus, if COA's processing of personal information, i.e. access to BSP's employee directory, is not necessary to its constitutionally mandated functions, such processing should therefore be anchored on any of the criteria for lawful processing as stated in Section 12 and Section 13 of the DPA for personal and sensitive personal information, respectively.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-003

15 January 2018

[redacted]

RE: VISITOR LOGBOOK

Dear [redacted]

This pertains to your query received by the National Privacy Commission (NPC) via NPC's official Facebook page. Particularly, you inquired about the following:

1. Appropriate means to regulate the visitor logbooks for security purposes;
2. Whether consent is needed in collecting personal information; and
3. Registration of the logbook with the NPC.

In your inquiry, you have mentioned that for every visitor entering the building or office, you require them to provide certain information in the logbook, such as: (1) name; (2) time of arrival; (3) time of departure; and (4) signature, and visitors are likewise required to surrender one (1) government-issued identification card, in exchange for the visitor's pass.

These information are considered as personal and sensitive personal information under the Data Privacy Act of 2012 (DPA).[1] Specifically, the name and signature of the individual or visitor are considered as personal information. 2 On the other hand, the government-issued identification card containing the number specifically assigned to the individual by the issuing government agency is considered as sensitive personal information.[3]

Given that you are processing personal and sensitive personal information as mentioned above, the DPA then directs you, as the personal information controller, to comply with duties and responsibilities under the law and implement appropriate security measures to ensure the protection and security of such personal data.[4]

---

[1] Republic Act No. 10173, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and in the Private Sector, Creating for this purpose a National Privacy Commission and for other purposes, "Data Privacy Act of 2012" (15 August 2012).
[2] Id., §3(g).
[3] Id., §3(l).
[4] Id., §21.

It is imperative to determine whether the information being collected in the logbooks are necessary and proportionate to the purpose of collection. Following such determination, the risks and vulnerabilities in the processing should likewise be identified and addressed, and an evaluation of the current security measures being implemented should be made to see if these are reasonable and appropriate to ensure the security and protection of personal information or whether there is a need to improve current practices. These may be accomplished through the conduct of privacy impact assessment.

To observe the principle of transparency to the data subjects, a privacy notice or privacy statement may be displayed alongside the logbook to apprise the visitors of the purpose of collection, recipients of collected information and retention period of stored information, among others.

Kindly note that Singapore's data protection authority, the Personal Data Protection Commission (PDPC), has decided a complaint in relation to the failure by a security company to safeguard their visitor logbook which resulted to a data breach incident.[5] The PDPC ruled that the recording and safekeeping of logbooks were considered as activities involving processing of personal data, hence, actual processes, practices and policies must be put in place in order to protect personal data and ensure the safety of the logbook at all times.[6]

With regards to consent of data subjects, a personal information controller may lawfully process personal information if the circumstance falls under any of the criteria for lawful processing of personal information, consent being one of them.[7] Legitimate interest is also a criterion for processing personal information. Please refer to Section 13 of the DPA for the criteria for lawful processing of sensitive personal information.

On the registration requirement, NPC issued a circular – Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making,[8] Section 5 of which provides:

> "SECTION 5: Mandatory Registration. A PIC or PIP shall register its data processing system if it is processing personal data and operating in the country under any of the following conditions:
>
> A. The PIC or PIP employs at least two hundred fifty (250) employees;

[5] Investigation under Section 50(1) of the PDPA 2012 and MCST 3696. Eagle Eye, Case Number: DP-1610-B0275, 29 June 2017. Available at https://www.pdpc.gov.sg/docs/default-source/enforcement-data-protection-cases/grounds-of-decision---eagle-eye---290617.pdf?sfvrsn=2. (Last accessed 13 December 2017)
[6] Id.
[7] Supra note 1, §12.
[8] See NPC Circular No. 2017-01

B. The processing includes sensitive personal information of at least one thousand (1,000) individuals;

C. The processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:

1. Information that would likely affect national security, public safety, public order, or public health;
2. Information required by applicable laws or rules to be confidential;
3. Vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exits in the relationship between a data subject and PIC or PIP;
4. Automated decision-making; or
5. Profiling

D. The processing is not occasional: Provided, that processing shall be considered occasional it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional."

Thus, if you satisfy any of the above-mentioned conditions, you are required to register with the NPC. For Sections 5(C) and (D) above, please note also the Appendix to the circular providing for the initial list of specific sectors, industries, or entities that shall be covered by mandatory registration.

It is important to note that the definition of a data processing system[9] includes manual or paper-based systems, i.e. logbooks, as well as electronic systems.

Finally, we wish to emphasize that data collection through visitor logbooks may often be overlooked. But as this a paper-based processing system, security measures to protect the data need not be a complicated matter as this will entail reasonable and appropriate organizational and physical security measures only.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[9] Implementing Rules and Regulations (IRR) of the RA No. 10173, §3(e).

ADVISORY OPINION
NO. 2018-004

22 January 2018

[redacted]

Re: EMPLOYEE NON-DISCLOSURE UNDERTAKING

Dear [redacted]

This pertains to your letter request for the review of the Philippine Institute for Development Studies' (PIDS) proposed Non-Disclosure Undertaking for its officials and employees in relation to its compliance with Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), and its Implementing Rules and Regulations (IRR).[2] A copy of the draft Non-Disclosure Undertaking provided is attached herewith as Annex "A."

At the outset, the DPA aims to protect individual personal information being processed by both the public and private sectors. Processing of personal information covers several activities, including but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[3] PIDS, as a nonstock, nonprofit government corporation,[4] is necessarily subject to the provisions of the DPA when it processes personal information in the course of its research,[5] dissemination and research utilization,[6] and outreach programs.[7]

Upon a review of the draft Non-Disclosure Undertaking, please see comments below:

---

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).
[3] Data Privacy Act of 2012, §3(j).
[4] About Us, Philippine Institute for Development studies, https://www.pids.gov.ph/about-us (last accessed 16 January 2018).
[5] Research Projects, https://www.pids.gov.ph/research-projects (last accessed 22 January 2018)
[6] Publications, https://www.pids.gov.ph/publications (last accessed 22 January 2018)
[7] Legislative Inputs (Comments on Proposed Bills), https://www.pids.gov.ph/legislative-inputs (last accessed 22 January 2018)

Employee Non-Disclosure Undertaking	Remarks
That I am fully aware and clearly understand that my access to the data, information and records (all hereinafter referred to as information) in the course of my functions as employee of the Philippine Institute for Development Studies is limited to my need for the information in the performance of my duties and responsibilities.	We understand that the information referred to herein is not actually limited to personal information[8] or sensitive personal information[9] as defined under the DPA. As such, there may be a need to clarify this by defining the term "information". Likewise, instead of referring solely to "access" you may opt to encompass other processing activities, i.e. "collection, access, use, disclosure or other processing necessary" for the performance of official functions and/or the provision of a public services.
That I will use my authorized access to the data only in the performance of my responsibilities of my position.	For consistency to the first undertaking above, consider using the term "information" instead of "data". Also, on authorized access, consider adding a provision or reference to the issuance of a security clearance[10] as this is required for purposes of providing access to personal data.
That I shall comply with all control established by the Philippine Institute for Development Studies regarding the use of information/data/material gathered/generated/collected.	To be more specific, you may use "access control policy" and/or "acceptable use policy" and any other applicable policy/ies instead of using "control".
That I shall be guided by the applicable PIDS policy and the National Privacy Commission rules, regulations and advisory and the provisions of RA 10173 and its Implementing Rules and Regulations. That I understand and agree that my obligation not to disclose information will continue even after I leave the employment with PIDS.	Consider adding a catch-all statement for guidance: "…its Implementing Rules and Regulations, and *any other applicable laws governing confidentiality of information*."

[8] RA No. 10173, §3(g) – 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.

[9] Id., §3(l) - 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 person, 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 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

[10] See: IRR of RA No. 10173, §31(a) and NPC Circular No. 2016-01, §15

I will exercise care to protect the data against accidental or unauthorized access, modifications, disclosures, or destruction.	To emphasize the significance of the officers and employees' role in data protection, further revision of this stipulation is recommended in such a manner that the officer or employee shall exercise "due diligence"[11] as defined under the law and prevailing jurisprudence.
I understand that any violation of this undertaking or other PIDS policies related to the appropriate release or disclosure of information may result in one or more sanctions including immediate termination of my access to data, disciplinary actions up to and including dismissal from employment, criminal penalties, or civil liability.	Sanctions should include revocation of the security clearance to access information.
I affirm that I have been given the opportunity to review and understand the PIDS Guidelines on Data Protection and other PIDS policies referenced therein, and I further affirm that my questions about those policies have been answered to my satisfaction.	Note that in the conduct of NPC's compliance checks, it is possible for the Commission to interview officials and employees and ask them regarding the company's policies and data processes. Thus, it is incumbent upon the company to make sure that officials and employees have indeed been briefed on said policies and processes and have a working understanding of the same. Finally, we wish to emphasize that a mandatory, agency-wide annual training on privacy and data protection policies is required to be conducted, and a similar training should be provided during all agency personnel orientations.[12]

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[11] See R.A. No. 386, otherwise known as the "Civil Code of the Philippines," Article 1163: Every person obliged to give something is also obliged to take care of it with the proper diligence of a good father of a family, unless the law or the stipulation of the parties requires another standard of care.
[12] NPC Circular No. 2016-01, §4(D)

ADVISORY OPINION
NO. 2018-005

05 February 2018

[redacted]

Re: DATA SHARING AGREEMENT/ DATA PROTECTION OFFICER

Dear [redacted],

This refers to your query received by the National Privacy Commission (NPC) via email. You stated that your company, Doxcheck, is involved in the online verification of documents through your website and mobile app.

We understand that the "Doxcheck Document Security System provides a secure and verifiable technology in the protection of documents. The system boasts multi-tier safeguards and a robust uptime of at least 99.9%. The secure, and flexible system is hosted on a distributed cloud architecture. This enables institutions to immediately and reliably protect and verify high-value documents 24/7."[1]

Specifically, your questions pertain to the following:

a. Is Doxcheck required to submit its data sharing agreements to the NPC for approval? and
b. Is the Data Protection Officer (DPO) position a different job title/ position in the company or can one person have two positions/ titles in the company?

Data Sharing Agreement vis-à-vis Outsourcing Agreement

The Implementing Rules and Regulations (IRR) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA), lays down the principles for data sharing[2] and outsourcing.[3]

[1] FAQs, https://www.doxcheck.com/faqs/ (last accessed 30 January 2018).
[2] IRR of RA No. 10173, §20.
[3] Id., §43-44.

To clarify, data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or personal information processor (PIP). In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.[4]

Our understanding of the processing activities of Doxcheck is that it provides "a unique DOXCHECK Global Code is assigned to every document using a 2048-bit data security encryption."[5]

The protected document itself is issued by "any institution/organization that issues high value documents such as: IDs, Birth Certificates, Training Certificates, Diploma, Transcript of Records, Membership Certificates, Membership Cards, Certificate of Employment, Medical Certificates, Authorization Letter, Good Moral, Any High Value Documents."[6]

Hence, Doxcheck is a PIP to whom PICs outsourced the processing, i.e. security and protection, of the documents which may contain personal data.[7]

Section 44 of the IRR provides that processing by a PIP shall be governed by a contract or other legal act that binds the PIP to the PIC. This agreement for outsourcing is not required to be submitted to the NPC for its approval prior to its execution. Note however that said document may be required for submission by the NPC in case of a compliance check or an investigation.

In the same manner, the IRR does not require the submission of data sharing agreements to the NPC for its approval. Bear in mind, however, the IRR requires, among others, that such data sharing agreements shall be subject to the review by the NPC, on its own initiative or upon complaint of the data subject concerned.[8] Hence, the NPC has the right to require the submission of such data sharing agreements should it deem necessary.

---

[4] IRR of RA No. 20173, §3(f).
[5] FAQs, https://www.doxcheck.com/faqs/ (last accessed 30 January 2018).
[6] Id.
[7] RA No. 10173, §3(i).
[8] IRR of RA NO. 10173, 20(b)(2)(b).

Data Protection Officer

As regards your query on the DPO, the NPC issued NPC Advisory No. 2017-01 – **Designation of Data Protection Officers** which sets out the guidelines on the designation of a DPO applicable to all who are engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR and the issuances of the NPC.

Pursuant to said Advisory, a DPO should be a full-time or organic employee of the PIC or PIP, occupying a regular or permanent position. To fully carry out the spirit and purpose of the law, the DPO shall act independently in the performance of his or her functions and shall enjoy sufficient degree of autonomy.

In his or her capacity as DPO, he or she may perform (or be assigned to perform) other tasks or assume other functions, however, such tasks and functions should not give rise to any conflict of interest.[9]

Given the foregoing, an individual currently holding a position within the company may be designated as the DPO. However, it is paramount that his or her tasks or functions do not give rise to any conflict of interest against the responsibilities of a DPO.

Note that the company is not precluded from creating a separate position for the DPO, or even a distinct Data Protection Office, should it determine that the same is reasonable and appropriate vis-à-vis the risk of its processing operations.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[9] NPC Circular No. 2017-01, "Conflict of Interest" refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO. This includes, inter alia, holding a position within the PIC or PIP that leads him to determine the purposes and the means of the processing of personal data. The term shall be liberally construed relative to the provisions of this Advisory.

ADVISORY OPINION
NO. 2018-006

06 February 2018

[redacted]

RE: CONSENT OF DATA SUBJECT PRIOR TO RELEASE OF SCHOOL RECORDS BY THE LYCEUM OF THE PHILIPPINES UNIVERSITY (LPU)

Dear [redacted]

This pertains to your inquiry received by the Privacy Policy Office of the National Privacy Commission (NPC) on 25 January 2018, which sought to clarify whether the regulation of the University Registrar of the Lyceum of the Philippines (LPU) on the release of school records is in consonance with the provisions of Republic Act No. 10173[1], also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances.

In your letter, you stated that you have requested information regarding your biological father from the LPU Registrar and the Alumni Affairs Office, specifically the following information: a) middle name; b) last registered address; and c) parents' names. We understand that you will use these information in relation to your personal search of your father whom you have not seen since you were a child.

First and foremost, LPU, as an educational institution, is considered as a personal information controller[3] (PIC), processing[4] personal information[5] of its students, employees, and alumni, thus, is covered by the law and under the jurisdiction of the NPC. The information that you requested

[1] AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIACY COMMISSION, AND FOR OTHER PURPOSES, "Data Privacy Act of 2012" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).
[3] Supra note [1], §3(h) - Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.
[4] Id., §3(j) – Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data
[5] Id., §3(g) - 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

are well within the definition of personal information in Section 3 of the DPA and are then subject to its rules and regulations.

As a PIC, LPU is bound to implement reasonable and appropriate organizational, physical, and technical measures to protect the personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.6 It is accountable for any personal information under its control and custody, including those transferred to a third party.[7]

Given the responsibility of LPU to secure personal information, its denial of your request for information may be justified due to the lack of consent of the data subject. Although consent is not the only condition for lawful disclosure[8] or processing, in general, of personal information, it may be the most appropriate criterion in this scenario.

Likewise, LPU as the PIC is mandated to recognize and enforce the rights of the data subject[9], including the right to be informed regarding the recipients to whom data will be disclosed. Thus, the data subject, your biological father, must be informed, and most importantly, approve of the disclosure of his personal information to you.

We truly understand your plight. However, this agency is mandated to protect the personal information of the data subjects from any unauthorized disclosure. Considering your purpose, LPU may not be the proper institution to provide you with the needed information. It is best to consider other avenues for your search.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[6] Id., §20.
[7] Id., §21.
[8] Supra note, §12.
[9] Id., §16.

ADVISORY OPINION
NO. 2018-007

26 February 2018

[redacted]

RE: DISCLOSURE OF THE MASTER LIST OF STUDENTS AND INDIVIDUALS WHO WERE VACCINATED WITH DENGVAXIA

Dear [redacted]

This pertains to your request for advisory opinion received by the Privacy Policy Office of the National Privacy Commission (NPC) on 05 February 2018, which sought to clarify whether the Department of Health (DOH) could provide a copy of the master list of students and individuals who were vaccinated with Dengvaxia®, without violating the provisions of Republic Act No. 10173[1], also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances.

In your letter-request, you have stated that the Public Attorney's Office (PAO) is seeking to obtain the following personal information for each of the children/individuals vaccinated, starting with those given in April 2016 for the purpose of extending free legal assistance in civil, criminal and administrative cases to all possible victims of Dengvaxia® related injuries, illnesses and deaths:

a. Name;
b. Birthday;
c. Home address;
d. Name of parents;

---

[1] AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIACY COMMISSION, AND FOR OTHER PURPOSES, "Data Privacy Act of 2012" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

e. Consent form;
f. Vaccination card;
g. Name of the vaccinator;
h. Position of the vaccinator; and
i. Health educator.

Furthermore, the same master list was requested by certain private organizations, i.e. Volunteers against Crime and Corruption (VACC), and some members of the media.

It is important to establish that the personal information sought to be collected by the PAO, VACC, and the media is considered as sensitive personal information as defined in Section 3(l) of the DPA, particularly those relating to the individual's age, health and health record (vaccination card, and status of being vaccinated). The information also relates to a vulnerable group of data subjects—minors.

In general, processing of sensitive personal information is prohibited by law except in the cases provided under Section 13 of the DPA. The release of "a copy of the master list of students and individuals who were vaccinated with Dengvaxia®" will be lawful processing if is provided for by existing laws and regulations, or has the consent of data subjects or authorized representatives, otherwise the processing might be considered as unauthorized processing under the Data Privacy Act.

The Commission is mindful that information provided to government or public authority may be processed without consent when it is done pursuant to the particular agency's constitutional or statutory mandate, and subject to the requirements of the DPA. In this case, the information sought to be released were not provided to the Public Attorney's Office, and were not collected for purposes of the PAO's legal mandate.

Under Republic Act No. 9406, it is our understanding that the mandate of PAO is to extend free legal assistance to indigent persons in criminal, civil, labor, administrative and other quasi-judicial cases. Should PAO then be authorized as legal representatives of the minor data subjects, they may then be provided information regarding the particular data subject they are representing, subject to the presentation of proof of such authorization.

We take time to emphasize that the government is one of the biggest repositories of the personal data of citizens. The government or its agencies, however, do not have the blanket authority to access or use the information about private individuals under the custody of another agency.

In all cases, the processing of personal data by any personal information controller, like the DOH or the PAO when expressly authorized by the data subject or by law, should always adhere to the general data privacy principles of transparency, legitimate purpose and proportionality.[3] Aside from this, personal information controllers should implement appropriate security measures for data protection. Moreover, before any personal information is transferred from one agency to another, it is highly recommended that the agencies execute a Data Sharing Agreement to ensure that there are adequate safeguards for data privacy and security implemented by both parties.[4] Kindly refer to NPC Circular No. 2016-02 – Data Sharing Agreements Involving Government Agencies for additional information.

Lastly, as to the request of the media and other private organizations, the disclosure of statistical or aggregated information without involving any personal or sensitive personal information should suffice. The release of a copy of the master list of students and individuals who were vaccinated with Dengvaxia®, which contains sensitive personal information to the Requesting, to any requesting public, could constitute an unwarranted invasion of personal privacy.

We urge the DOH to be circumspect in releasing information relating to sensitive personal information of individuals. It should do so only if it is satisfied that such release is authorized under law, adheres to data privacy principles and reasonable and appropriate security measures are in place for the protection of said data. In order to fulfill its own mandate, the DOH collects health information of the Filipinos, who should be able to trust that their information will be protected and used only for the purpose by which they are collected.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[3] Supra note 2., §18.
[4] Supra note 2., §22(d).

ADVISORY OPINION
NO. 2018-008

02 April 2018

[redacted]

Re: SUBMISSION OF EMPLOYEE NAMES AND SALARY RECEIVED IN CY 2017 FOR ISSUANCE OF COMMUNITY TAX CERTIFICATE (CTC)

Dear [redacted],

This pertains to your updated inquiry via email, received by the Privacy Policy Office of the National Privacy Commission (NPC) on 19 February 2018, which sought to clarify whether the employer's disclosure of the list of employees with their corresponding salary in CY2017 to the Office of the City Treasurer City is in consonance with the provisions of Republic Act No. 10173[1], also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances.

To backtrack, there was an initial email inquiry dated 11 January 2018 where it was mentioned that the City of Dumaguete was requesting for employee information (name, address and educational attainment) as a new requirement for business permit renewal. We thereafter sent a clarificatory letter and requested for further information on the said requirement.

In your email dated 13 February 2018, you attached copies of the following:

1. Letter from the Office of the City Treasurer of Dumaguete City dated 6 February 2018 informing the manager of SPI-CRM of the requirement for all employees to secure and pay their community tax, and for that purpose, to prepare a list of all employees with their

[1] AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIACY COMMISSION, AND FOR OTHER PURPOSES, "Data Privacy Act of 2012" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

corresponding annual salary for 2017, and finally, to coordinate on the possible appointment date and time for the representative of the City Treasurer's Office to come and visit the establishment to personally issue the community tax certificates (CTCs) to the employees;

2. Your email sent to the City Treasurer of Dumaguete City on 8 February 2018 wherein you forwarded NPC's letter requesting for clarification and further information; and
3. Letter from the Office of the City Treasurer of Dumaguete City dated 12 February 2018 expounding on the requirement for the list of all employees with their corresponding annual salary for 2017 as a basis for the computation of the community tax.

Community Tax

Section 157 of the Local Government Code (LGC) provides as follows:

> "SECTION 157. Individuals Liable to Community Tax. - Every inhabitant of the Philippines eighteen (18) years of age or over who has been regularly employed on a wage or salary basis for at least thirty (30) consecutive working days during any calendar year, or who is engaged in business or occupation, or who owns real property with an aggregate assessed value of One thousand pesos (P1,000.00) or more, or who is required by law to file an income tax return shall pay an annual community tax of Five pesos (P5.00) and an annual additional tax of One peso (P1.00 for every One thousand pesos (P1,000.00) of income regardless of whether from business, exercise of profession or from property which in no case shall exceed Five thousand pesos (P5,000.00)."

The above is implemented by the City of Dumaguete under their own Local Tax Code, Sections 89 and 90 of Ordinance No. 125.[3]

We understand that the list of all employees with their corresponding annual salary for 2017 is being requested by the Office of the City Treasurer for submission prior to the actual visit of the representative of said office for purposes of facilitating the efficiency of the transaction, i.e. to enable them to prepare and print the CTCs beforehand, ready for signature and thumbprinting of the respective employees.

Upon evaluation, the personal information being requested by the Office of the City Treasurer satisfies the general data privacy principles of transparency, legitimate purpose and proportionality.[4]

---

[3] Letter from the Office of the City Treasurer of Dumaguete City dated 12 February 2018

First, the collection and processing of personal information is pursuant to a statutory mandate.[5] Second, there is an assurance that the personal information collected will be stored securely and kept confidential.[6] Third, the information requested are relevant and necessary to enable the Office of the City Treasurer to accurately compute and determine the community tax to be collected from every employee.[7]

However, if the request of preliminary submission of the names and salaries of employees is purely for efficiency purposes, the Office of the City Treasurer may opt to just give out handwritten CTCs instead of having it pre-printed. The representative may perform the calculation of the taxes to be paid during the appointment period where the employees would be required to present their respective BIR Form No. 2316 - Certificate of Compensation Payment/Tax Withheld as proof of their annual salary for 2017.

We note also that it is possible that some of the employees may have already paid their community tax and have been issued with the CTCs for 2018. Hence, the collection of personal information of those employees is unnecessary.

Consequently, you, as employer, must inform the employees of the appointment schedule with the representative from the Office of the City Treasurer in order for them to have ample time to prepare the payment and documents necessary for the issuance of the CTC.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC – Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[4] Implementing Rules and Regulations of RA No. 10173, §17 and 18.
[5] Id.
[6] Id.
[7] Id.

ADVISORY OPINION
NO. 2018-009

01 March 2018

[redacted]

Re: DISCLOSURE OF PERSONAL INFORMATION TO THE PHILIPPINE ARMY

Dear [redacted]

This is in response to your letter received by the National Privacy Commission (NPC) on 16 January 2018 with regard to the request of the 97th Military Intelligence Company of the 9th Infantry Division of the Philippine Army for submission of the updated Media Profile Report, which contains personal information of media persons in Albay.

Specifically, the following information are requested:

1. Name of Station;
2. Owner/Station Manager;
3. News Program/Title;
4. Airing Time;
5. Anchor/News Carter; and
6. Contact Number.

We understand that the above information will be forwarded to higher headquarters and will serve as basis or guide to the incoming new Commander of the 9th Infantry Division of the Philippine Army.

Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), states that the processing of personal information shall be allowed, subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public and in adherence to the principles of transparency, legitimate purpose and proportionality.[2]

[1] AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIACY COMMISSION, AND FOR OTHER PURPOSES, "Data Privacy Act of 2012" (15 August 2012).
[2] Id., §11.

Furthermore, Section 12(e) thereof provides for one criterion for lawful processing of personal information, to wit:

> "(e) the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;" (underscoring supplied)

In relation to the above, the 1987 Constitution states that the mandate of the Armed Forces of the Philippines (AFP) to protect the people and the State and to secure the sovereignty of the State and the integrity of the national territory.[3]

Specifically, the 1987 Administrative Code provides that the Philippine Army shall be responsible for the conduct of operations on land,[4] and has the following functions:

1. Organize, train and equip forces for the conduct of prompt and sustained operations on land;
2. Prepare such units as may be necessary for the effective prosecution of the national defense plans and programs and armed forces missions, including the expansion of the peacetime army component to meet any emergency;
3. Develop, in coordination with the other Major Services, tactics, techniques and equipment of interest to the army for field operations;
4. Organize, train and equip all army reserve units; and
5. Perform such other functions as may be provided by law or assigned by higher authorities.[5]

As stated in the letter request, the 97th Military Intelligence Company is a support unit which assists in the development of contingency plans and concepts by providing information to maintain peace and order in the Province of Albay.

While the DPA recognizes such mandate, the law is categorical in stating that the processing of personal information must adhere to the principles of transparency, legitimate purpose and proportionality. Personal information must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably

---

[3] See: 1987 Philippine Constitution, Article II, §3.
[4] Executive Order No. 292, Title VIII, Subtitle II, Chapter 8, §48.
[5] Id., §49.

practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only.[6]

Hence, it may be prudent to ask for further clarification on the specific purpose of the request for the Media Profile Report as there is no explicit statement in the letter request as to the purpose thereof.

Moreover, the disclosure of personal information to the 97th Military Intelligence Company should adhere to the principle of proportionality.[7] An evaluation of the personal information required to be disclosed vis-a-vis its intended purpose should be done to ensure that it is adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Finally, it should be noted that the data subjects such as the individual owners and/or station managers and anchors whose personal information will be disclosed should be informed of the same, including what personal information will be submitted, in relation to their right to be informed under the DPA and its IRR.[8] The NTC may choose to include a statement on these types of disclosures or submissions through its Privacy Policy.

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 the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[6] RA No. 10173, §11(a).
[7] See: IRR of RA No. 10173, §18(c).
[8] See: IRR of RA No. 10173, §34(a).

ADVISORY OPINION
NO. 2018-010

4 May 2018

[redacted]

RE: PRECINCT FINDER AND COMELEC MINUTE RESOLUTION NO. 17-0715

Dear [redacted],

This pertains to your letter received by the Privacy Policy Office of the National Privacy Commission (NPC) on 27 February 2018, requesting for an opinion on whether the alternative precinct finder of the COMELEC is compliant with Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA).

We understand that the Precinct Finder search facility in the COMELEC website was made temporarily unavailable to the public after the 2016 National and Local Elections (NLE). Thereafter, the following undertakings were completed:

1. The source code of the Precinct Finder used for the 2016 NLE was audited and cleared for public access by the Department of Information and Communications Technology (DICT); and
2. The COMELEC's Information Technology Department (ITD) made an enhancement of the Precinct Finder by deleting the following voter information:
   a. Date of birth
   b. Residential address; and
   c. Voter's ID availability status.

We understand further that should the COMELEC decide to use the enhanced Precinct Finder, the source code would have to undergo DICT audit which may take more than one year.

---

[1] 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" (15 August 2012).

Hence, the following recommendations were put forward, taking into consideration the May 2018 Barangay and Sangguniang Kabataan Elections (BSKE):

1. Use the enhanced Precinct Finder if the source code review and audit are completed before May 2018;
2. If the audit is not completed on time:
    a. The Precinct Finder intended for the 2016 NLE shall be used as it has already passed DICT assessment with the same number of data fields; or
    b. The Precinct Finder will not be implemented and COMELEC will announce the unavailability of the facility in the website.

Another proposed alternative pursuant to COMELEC Minute Resolution No. 17-0715 is the posting of the name of the registered voter with the precinct number in the COMELEC website for the 2018 BSKE. You inquire on whether this last alternative is compliant with the DPA.

Bearing in mind the personal data breach in 2016 which involved the COMELEC website database and affected millions of voter registration records, the last alternative of simply posting of the name of the registered voter with the corresponding precinct number in the website for the 2018 BSKE is the most suitable alternative.

As the primary purpose of the Precinct Finder facility is to enable the registered voters to know their specific precinct numbers, any additional fields of personal data, i.e. date of birth, gender, address, civil status, voter identification number, etc., is unnecessary for that specific purpose.

Personal information controllers, such as the COMELEC, should be mindful that the processing of personal data should always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Specifically, the principle of proportionality declares that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[2]

Recalling the NPC's decision in NPC Case No. 16-001:[3]

> "... COMELEC is no ordinary data controller; it is effectively one of

---

[2] Implementing Rules and Regulations (IRR) of RA No. 10173, §18(c).
[3] In re: Investigation of the security incident involving COMELEC website and/or data processing system, NPC Case No. 16-001, 28 December 2016.

the Philippines' largest data controllers. The COMELEC creates, maintains, and processes data to establish a clean, complete, permanent, and updated list of voters, through the adoption of biometric technology, for use in national and local elections.

xxx xxx xxx

The numbers are staggering: there were a total of 76,678,750 voter registration records affected. Although the sensitive fields of these records were not shown to the public, the website database contained sensitive personal information not necessary for the purpose for which the data is being processed."

Personal data in the Precinct Finder facility should be limited to those which are absolutely necessary for the specified purpose of said search facility. Pursuant to the practice of data minimization, COMELEC should identify the minimum amount of personal data needed to properly fulfill the Precinct Finder's purpose.[4]

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[4] See: Information Commissioner's Office, The amount of personal data you may hold (Principle 3), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/ (last visited 28 February 2018)

ADVISORY OPINION
NO. 2018-011

22 March 2018

[redacted]

RE: DISCLOSURE OF THE UNIT NUMBERS OF THE MEMBERS OF A CONDOMINIUM ASSOCIATION

Dear [redacted]

This pertains to your request for advisory opinion received by the Privacy Policy Office of the National Privacy Commission (NPC) on 23 February 2018, which sought to clarify whether the disclosure of unit numbers of the members of the Olympic Heights Condominium Association, Inc. (Olympic) for purposes of the determination and verification of the existence (or non-existence) of a quorum would violate the provisions of Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances of the NPC.

In your email, you stated that you are a member in good standing of Olympic, which is a non-stock, non-profit corporation. On 10 February 2018, Olympic had its General Assembly where it was declared that there was no quorum.

You thereafter requested for the list of the unit numbers of the members in good standing and those who are delinquent for purposes of verifying the above conclusion as to the lack of quorum during the General Assembly. However, the lawyer of Olympic denied such request, claiming that revealing the unit numbers will lead to personal information, and therefore should not be allowed.

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

It is worthy to note that the unit numbers of a condominium may be considered as personal information[3] as these may represent and correspond to the natural persons who are the registered owners of that particular condominium unit. The condominium association, as the entity holding and recording all information pertaining to the registered unit owners, can easily identify the individual owners of the condominium unit. Nevertheless, contrary to the position of the lawyer of the association, Section 12 of the DPA provides for the criteria for lawful processing of personal information.

Particularly, Section 12(c) states that personal information may be processed if it is necessary for compliance with a legal obligation to which the personal information controller is subject. In your case, the condominium association has a legal obligation, rooted in Section 74 of the Corporation Code, to provide access to and inspect corporate records and documents, even the financial statement, as stated in Section 75 of the same Code.

The DPA has the twin task of protecting the fundamental human right of privacy while ensuring free flow of information.[4] The DPA does not operate to curtail existing rights of members of a condominium corporation, specifically on inspection of corporate books and records, subject to existing laws and regulations on such matters.

Hence, the condominium corporation may lawfully disclose the unit numbers of the members of the association based on the DPA and your right to inspect the books and records of the corporation as discussed above. Although the right to inspect is subject to certain limitations, such may be raised as a defense in actions filed under Section 74 of the Corporation Code.[5]

Be that as it may, the more pertinent rules that shall govern your inquiry are the Corporation Code of the Philippines, Condominium Act, Securities Regulation Code, and other related laws, as well as the Articles of Incorporation and By-Laws of Olympic. We understand that these may provide information on the conduct of members' regular or special meetings, quorum in meetings, and determination of voting rights of each member, as well as rights of members as to inspection and access to the association's corporate books and records.

---

[3] Supra note 1, §3(g)- "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.
[4] Supra note 1, §2.
[5] Philippine Associated Smelting and Refining Corporation vs. Pablito O. Lim, et. al., G.R No. 172948 (05 October 2016).

We understand further that the request for inspection is rooted in matters involving the failure to elect a new set of trustees and/or officers and other controversies existing between the members and the trustees and/or officers of Olympic. These concerns are purely intra-corporate[6] in nature and pursuant to the applicable laws on the matter, these intra-corporate disputes fall under the jurisdiction of the proper Regional Trial Court.[7] Please direct your subsequent efforts in resolving these matters in the proper forum.

This opinion is based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC – Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[6] SEC-OGC Opinion No. 17-10 (31 August 2017).
[7] See: Presidential Decree No. 902-A, §5, in relation to the Securities Regulation Code, §5.2.

ADVISORY OPINION
NO. 2018-012

02 April 2018

[redacted]

RE: RELEASE OF SERVICE RECORD

Dear [redacted],

This pertains to your request for advisory opinion received by the Privacy Policy Office of the National Privacy Commission (NPC) on 01 March 2018, which sought to clarify whether the National Transmission Corporation (TransCo) can lawfully release the service records of former employees for the processing of their claims, as a result of the case filed by the National Power Corporation (NAPOCOR) Drivers and Mechanics Association (DAMA). Also, whether the consent of the employees is required for the said purpose.

At the outset, it is important to establish that the respondents in the DAMA case are former employees of the NAPOCOR, a government-owned and controlled corporation, created under Commonwealth Act No. 120.[1]

Section 4 of Republic Act No. 10173,[2] also known as the Data Privacy Act of 2012 (DPA), provides that the law does not apply to information about officers or employees of government institutions, particularly relating to the position or function of such individual, including the classification, salary range and responsibilities of the position held by such employee. The exemption is only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.

---

[1] AN ACT CREATING THE "NATIONAL POWER CORPORATION," PRESCRIBING ITS POWERS AND ACTIVITIES, APPROPRIATING THE NECESSARY FUNDS THEREFOR, AND RESERVING THE UNAPPROPRIATED PUBLIC WATERS FOR ITS USE (03 November 1936).

[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" (15 August 2012).

[3] Id., §12(c).

Furthermore, personal information may be lawfully processed when it is necessary for compliance with a legal obligation to which TransCo is subject.[3] In this case, we understand that TransCo is required to provide the service records of the respondents in order to fulfill the judgement of the court. Indeed, the judgment in the case will not be fully executed without information pertaining to the years of service of the employees, as well as the corresponding salary of the last position held.

Considering that there is a legal obligation to disclose the service records, TransCo can lawfully release the service records, even without the consent of the data subjects or employees, in this case.

However, although there is a legitimate purpose for the disclosure of service records, TransCo must ensure that the information to be disclosed is adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose, i.e. the proper computation and processing of claims.[4]

It is worthy to note that the DPA has the twin task of protecting the right to privacy and ensuring the free flow of information. The law cannot be used as an excuse to hinder the speedy administration of justice and execution of judgment, especially the disposition of this case which aims to compensate government employees for due and demandable claims.[5]

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC – Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

---

[4] Implementing Rules and Regulations of RA No. 10173, §18(c).
[5] Republic of the Philippines, et al., vs. Hon. Luisito G. Cortez, et al, G.R No. 187257 and Rolando G. Andaya vs. Hon. Luisito G. Cortez, et. al., G.R No. 187776 (07 February 2017).

ADVISORY OPINION
NO. 2018-013

18 April 2018

[redacted]

Re: PRIVACY POLICY AND CONSENT OF DATA SUBJECTS

Dear [redacted],

This refers to your inquiry received by the National Privacy Commission (NPC) via email. You sought for clarification on the compliance of an insurance company with the requirements of Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulation (IRR), in relation to a privacy policy submitted by the said insurance company pursuant to the requirement under Insurance Commission (IC) Circular Letter (CL) No. 2014-47 - Guidelines on Electronic Commerce of Insurance Products. A copy of the privacy policy is attached herewith as Annex "A."

We understand that upon evaluation conducted by the IC Regulation Enforcement and Prosecution Division and Information Systems Division, the submitted privacy policy of that insurance company is not compliant with the DPA for the reason being that the company shall be disclosing personal information of their customers to third party entities without the required customers prior written approval.

In addition, you mentioned that since this transaction is done electronically, and the customer will just click the agree/disagree portion provided for in the online transaction, you ask if this is considered compliant with the DPA.

[1] 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" (15 August 2012).

Privacy policy vs. Consent

At the outset, it must be clarified that the submitted "privacy policy" should be referred to as the company's privacy notice. A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[2] A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.[3]

Having stated that, there is also a need to determine and clarify the distinction between privacy policy and securing the consent of the data subject for the processing of his or her personal information.

Being a mere notice, it is emphasized that the privacy policy or notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects.

The principle of transparency adhered to by the DPA dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[4] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[5]

Thus, in line with the right to information of the data subject, personal information controllers (PICs) are required to apprise the data subject of the following:

1. Description of the personal data to be processed;
2. Purposes for processing, including: direct marketing, profiling, or historical, statistical or scientific purpose;
3. Basis of processing (legal or statutory mandate, contract, etc.)
4. Scope and method of processing;
5. Recipient/classes of recipients to whom the personal data are or may be disclosed;
6. Identity and contact details of the Personal Information Controller;

[2] IAPP, Glossary of Privacy Terms, available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2
[3] Id.
[4] IRR of RA No. 10173, §18(a).
[5] Id.

7. Retention period; and
8. Existence of rights as data subjects.

On the other hand, obtaining consent from the data subject for the purposes of processing his or her personal data is a different requirement altogether.

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 his or her personal, sensitive personal, or privileged information.

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic or recorded means.[6]

We reiterate that the mere posting of a PIC's privacy policy or notice and requiring the consumers to agree thereon via the online platform does not equate to obtaining the consent of the data subject for purposes of processing his or her personal information as required under the law.

While consent may be obtained through electronic means, the fact that the data subject must agree to a privacy policy or notice fails to meet the requirement of a meaningful consent. A "bundled" consent, for instance, will generally not suffice as the data subject is not empowered to make a true choice.

In addition, we refer to the IC's CL No. 2014-47 which provides for the requirement for consumers' consent as follows:

"8.5 Insurance providers shall not, as a condition of sale, require consumers to consent to the collection, use or disclosure of personal information beyond that is necessary to complete the sale.

8.6 When consumer's consent to the collection, use and disclosure of personal information is required, and cannot reasonably be implied, such consent shall be:

(a) Provided separately from consent to other terms and conditions of the insurance contract; and
(b) Provided through a clearly worded, online opt-in process.

[6] RA No. 10173, §3(b).

8.7 The consent of the consumer may also be included in the application or executed in a separate paper form." (underscoring supplied)

From the foregoing, the insurance company's privacy policy conforms to the requirements of the DPA and need not be revised.

Nonetheless, the IC may direct the insurance company to create a separate form or opt-in process in the online transaction for securing the consent of the consumers to the processing of his or her information, if consent is the proper basis for processing personal data.

For you reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-015

12 April 2018

[redacted]

Re: CONSENT REQUIREMENT ON OUTSOURCING AGREEMENT WITH AN EXTERNAL SERVICE PROVIDER

Dear [redacted]:

This is in response to your letter received by the National Privacy Commission (NPC) on 15 February 2018 regarding your request for clarification on whether the consent of employees is required for the engagement of an external provider for the analysis of the results of skills, personality, and behavior assessments in relation to provision of employee training and development programs and operationalization of workforce competency framework.

Outsourcing

The Implementing Rules and Regulations (IRR)[1] of Republic Act No. 10173,[2] otherwise known as the Data Privacy Act of 2012 (DPA), defines outsourcing as the disclosure of personal data by a personal information controller (PIC) to a personal information processor (PIP) [3] for the latter to perform processing activities as instructed by the former.

It is important to note that in an outsourcing agreement, the PIP does not have its own purpose for processing but merely carries out the instruction given by the PIC. Further, it cannot amend or process personal data outside the bounds of its agreement with the PIC. Hence, BSP should

[1] Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012 (24 August 2016).
[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" (15 August 2012).
[3] Supra note 1, §3(f).

be the one to determine the purpose and means of the processing and ensure that the external service provider will not process the personal data for its own purpose or any purpose outside that determined in the service agreement.[4]

Please note also that BSP remains responsible for personal information under its control or custody, which necessarily includes information that have been transferred to a third party for processing, whether domestically or internationally.

BSP is still accountable for complying with the requirements of the DPA and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.[5]

Consent

Whether processing is based on consent, law, or some other criteria for lawful processing, the PIC is not required to obtain a separate consent from the data subject before entering into an outsourcing agreement as the purpose of the processing remains to be the same and the PIC remains to be the same.

As such, if the consent of employees has already been obtained for processing of personal data related to human resource activities, a separate consent for the outsourcing is no longer needed. Also, the processing of personal information for employee training and development programs and operationalization of workforce competency framework could be considered as necessary and is related to the fulfillment of a contract between BSP as employer and its employees.

Nevertheless, considering the right of data subjects to be informed and notified of the processing of their personal data, the PIC must indicate in its privacy notice or privacy policy the particular data processing activities that are outsourced.[6] BSP may also use other means, such as through appropriate internal communications, to ensure that its employees are adequately informed of the processing involved under the outsourcing agreement.

---

[4] See: Implementing Rules and Regulations (IRR) of Republic Act No. 10173, § 44(b).
[5] See: Republic Act No. 10173, § 21(a) and IRR, Rule X.
[6] See: Republic Act No. 10173, § 16(a) and (b).

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-016

12 April 2018

[redacted]

RE: COMPLIANCE OF RESIDENT PHYSICIANS TO THE REQUIREMENT OF PROFESSIONAL SOCIETIES FOR DIPLOMATE BOARD EXAM AND ACCREDITATION

Dear [redacted]

This refers to your inquiry received by the National Privacy Commission (NPC) on 27 February 2018 regarding the compliance of your resident physicians with the requirements of the Philippine College of Surgery (PCS) and Philippine Obstetrics and Gynecology Society (POGS) for diplomate board exam and accreditation. We understand that one of the requirements is to submit a report on the actual cases that they have handled during their residency.

We understand further that some of these cases date back to January 2015 and were not covered by the revised consent for admission.

The information that the PCS and POGS require include the following:

1. Name of patient;
2. Date of admission;
3. Date of operation;
4. Hospital number; and
5. Attending physician/consultant.

You are seeking guidance on how Capitol Medical Center (CMC) can resolve the issue without violating Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), given that consent from the patients was not obtained by CMC.

[1] 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" (15 August 2012).

Criteria for lawful processing of personal data

The processing of personal, sensitive personal and privileged information (collectively, personal data) shall be allowed, subject to the compliance with the requirements of the DPA, and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.[2]

Specifically, personal data must be collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only, and processed fairly and lawfully.[3]

Given these requirements, the patient, as the data subject, should have been informed of the purpose of the processing of his or her data, and the processing thereof should be proportionate to the purpose.

CMC's disclosure of the patients' data for purposes of fulfilling the resident physicians' submission requirements for diplomate board exam and accreditation to the PCS and POGS may be allowed under the DPA provided that the patient has provided consent.[4]

The NPC understands that patients' personal data are necessary in order to avoid fraud cases. An option to consider is to pseudonymize the patients' data prior to disclosing the same. Pseudonymization consists of replacing one attribute (typically a unique attribute) in a record by another.[5] While pseudonymization lessens the risks, personal data which have undergone pseudonymization remains to be personal data,[6] hence, consent is still necessary.

In the event that the CMC can no longer obtain consent from the patients, there should be design methods and techniques wherein the PCS and POGS can validate that the cases handled by the resident physicians are true and correct without involving disclosure of personal data to the said professional societies. This may be in form of a certification from the CMC.

---

[2] RA No. 10173, §11. 3 RA 10173 § 11; IRR § 20 (b)
[4] RA No. 10173, 3(b) – 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.
[5] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.
[6] See: General Data Protection Regulation, recital 26

Another option is to anonymize the data. Note that the DPA is not applicable to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.[7]

We wish to emphasize that the DPA mandates that personal information controllers (PICs), such as CMC, must uphold the rights of data subjects and implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful disclosure, as well as against any other unlawful processing.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[7] Id.

ADVISORY OPINION
NO. 2018-017

12 April 2018

[redacted]

Re: TRADE SECRETS

Dear [redacted],

This pertains to your query received by the National Privacy Commission (NPC) via email. You seek to clarify whether trade secrets as recognized by jurisprudence as privileged communication falls under the scope of Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA).

The Supreme Court in Air Philippines Corporation vs. Pennswell, Inc.[2] thoroughly discussed what constitutes a trade secret, to wit:

> "A trade secret is defined as a plan or process, tool, mechanism or compound known only to its owner and those of his employees to whom it is necessary to confide it. The definition also extends to a secret formula or process not patented, but known only to certain individuals using it in compounding some article of trade having a commercial value. A trade secret may consist of any formula, pattern, device, or compilation of information that: (1) is used in one's business; and (2) gives the employer an opportunity to obtain an advantage over competitors who do not possess the information. Generally, a trade secret is a process or device intended for continuous use in the operation of the business, for example, a machine or formula, but can be a price list or catalogue or specialized customer list."[3]

---

[1] 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" (15 August 2012).
[2] Air Philippines Corporation v. Pennswell, Inc., 299 SCRA 744 (2007).
[3] Id., citations omitted.

By its very definition, trade secrets refer to information relating to plans, processes, tools and the like of a business. The DPA, on the other hand, was enacted to protect and secure personal data of individuals in information and communication systems in the government and in the private sector.[4] Personal data includes all types of personal information, i.e. personal information, sensitive personal information and privileged information, the latter referring to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.[5]

For the purposes of scope and protection under the DPA, the privileged information should constitute privileged communication under the Rules of Court and other laws, and relate to information about individuals.

Trade secrets that do not relate to individuals shall not fall under the scope of the DPA. However, as mentioned above, a specialized customer list may be a trade secret as well. If this involves a list of individual natural persons then the same may fall under the scope of the DPA as either personal or sensitive personal information, depending on what is included in such list or database.

Nonetheless, we note that jurisprudence has consistently upheld the privileged nature of trade or industrial secrets as an exemption from compulsory disclosure,[6] thus, the unwarranted or unauthorized disclosure thereof is already protected.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

---

[4] Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012, §2.
[5] Id., §3(q).
[6] Air Philippines Corporation; See also Mirpuri v. Court of Appeals, 376 Phil. 628 (1999) and Chavez v. Presidential Commission on Good Government and Magtanggol Gunigundo, 360 Phil. 133, 161 (1998).

ADVISORY OPINION
NO. 2018-018

12 April 2018

[redacted]

Re: PUBLICATION OF DECISIONS ON PHILHEALTH WEBSITE

Dear [redacted]:

This is in response to your request for opinion addressed to the Department of Information and Communications Technology (DICT) [redacted]. which was forwarded to and received by the National Privacy Commission (NPC) on 20 March 2018.

You inquired on whether the posting of decisions on the PhilHealth website under the proposed "CAAC Webpage" of administrative cases of health care providers appealed to and decided by the Committee on Appealed and Administrative Cases (CAAC) and the PhilHealth Board of Directors (Board), which may disclose patient and health information, is violative of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA).[1]

At the outset, it must be established that the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of personal information.[2] Processing includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[3]

---

[1] 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" (15 August 2012).
[2] See: Republic Act No. 10173, § 4.
[3] Id., §3(j).

We understand that during the course of the investigation, deliberation and resolution of an administrative case, the CAAC and the Board may be processing personal information of the patients and other interested parties.

Insofar as the health care provider[4] involved in a case decided by the CAAC and the Board is a (1) healthcare institution, (2) health maintenance organization (HMO), or (3) community-based health care organization (CBCHO), the corporate or business information pertaining to them, as entities, are not covered by the DPA since they are juridical persons. As such, processing of information pertaining to such juridical entities, including publication thereof, is not governed by the DPA.

On the other hand, as to the health care providers who are individuals, i.e. a health care professional, who is any doctor of medicine, nurse, midwife, dentist, pharmacist or other health care professional or practitioner duly licensed to practice in the Philippines and accredited by PhilHealth,[5] the processing of their information, which includes publication, of any proceeding for any offense committed or alleged to have been committed by such person and the disposal of such proceedings, is prohibited except in cases enumerated in Section 13 of the DPA.

Specifically, Section 13(b) of the DPA allows the processing of sensitive personal information when the same is provided for by existing laws and regulations and the statute does not require the consent of the data subject in processing the personal data. However, the regulatory enactment must guarantee the protection of the sensitive personal information being processed.

Also, as to the processing of personal data pertaining to patients involved in the resolution of cases, Section 13(b) of the DPA may likewise be applicable.

We recognize that the quasi-judicial provisions of the Implementing Rules and Regulations of RA No. 10606 requires the posting of decisions in the PhilHealth Corporate Website, to wit:

> "Section 141. Posting of Decisions in the PhilHealth Corporate Website.
> All Decisions of the Arbitration Office or the PhilHealth Board which have been deemed Final and Executory shall be posted in the PhilHealth Website."

---

[4] IRR of Republic Act No. 10606, § 3(y).
[5] Id., §3(y)(2)

The Board may thus publish its decisions which have become final and executory pursuant to the foregoing provision and in accordance with Section 13(b) of the DPA.

While the NPC recognizes such mandate, PhilHealth also has obligations under the principle of proportionality in relation to public disclosures of sensitive personal information. This principle requires that "the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means."[6]

With this, it is proper for the CAAC and the Board to judiciously evaluate and determine whether the publication of the decisions on the website is indispensable in achieving its purpose. The Board can consider redaction of sensitive personal information, such as the identity of patients and their health information, which may not be necessary for purposes of posting in the website.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

6 IRR of the DPA of 2012, § 13(c).

ADVISORY OPINION
NO. 2018-019

18 April 2018

[redacted]

RE: APPOINTMENT OF DATA PROTECTION OFFICER AND REGISTRATION OF DATA PROCESSING SYSTEM OF A HOMEOWNERS' ASSOCIATION (HOA)

Dear [redacted]

This pertains to your request for advisory opinion received by the Privacy Policy Office of the National Privacy Commission (NPC) on 15 March 2018, which sought to clarify whether HOAs are covered by Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances of the NPC. Particularly, whether they are required to appoint its own Data Protection Officer (DPO) and register its data processing system with the NPC.

Scope

It is important to recall that the DPA applies to all the processing of all types of personal information and to any natural and judicial person involved in personal information processing.[3]

Processing of personal data pertains to any operation or any set of operations performed upon such data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction.[4]

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).
[3] Supra note 1., §4.
[4] Id., §3(j).

Consequently, a HOA, being a juridical entity[5] engaged activities geared towards the provision of basic community services and facilities for its members-homeowners, may inevitably perform processing of personal information of its individual members-homeowners. It is considered as a personal information controller[6] (PIC) and is covered by the DPA.

It is of no matter that a HOA will not be dealing with the processing of sensitive personal information of persons other than its members. The DPA is applicable nonetheless, whether the personal data processed is from internal or external sources.

Appointment of a DPO

NPC Advisory No. 2017-01 dated 14 March 2017 on the Designation of Data Protection Officers (DPO) states that pursuant to Section 21(b) of the DPA and Section 50(b) of the IRR, PICs shall designate an individual or individuals who are accountable for the organization's compliance with the law.

The Advisory and the guidelines apply to all PICs and personal information processors[7] (PIPs) both in the government or private sector. The designation of a DPO is mandatory for PICs and PIPs, regardless of the number of employees, number of sensitive personal information processed, nature of processing or duration or regularity of processing activities.

Thus, the HOA is mandated to appoint a DPO to ensure the HOA's compliance with the DPA, its IRR and related issuances.

Registration of Data Processing Systems

NPC Circular No. 2017-01[8] dated 31 July 2017 regarding the registration of data processing systems provides that in line with Sections 46 and 47 of the IRR, a PIC or PIP that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, is not occasional, or includes sensitive personal information of at least one thousand (1,000) individuals.

---

[5] AN ACT PROVIDING FOR A MAGNA CARTA FOR HOMEOWNERS AND HOMEOWNERS' ASSOCIATIONS, AND FOR OTHER PURPOSES, "Magna Carta for Homeowners and Homeowners' Associations", Republic Act No. 9904 (07 January 2010), §4.
[6] RA No. 10173, §3(h).
[7] Id., §3(i).
[8] Id.

In your letter-request, you mentioned that HOAs are not likely to employ at least two hundred fifty (250) employees and will deal only with the processing of sensitive personal information of its members.

Note, however, that HOAs will be required to register its data processing system/s in the event of processing of sensitive personal data of at least one thousand (1,000) individuals or homeowners.

Thus, we recommend the conduct of a privacy impact assessment (PIA)[9] so that HOAs can make a determination and an inventory of the categories of data and exact number of data subjects whose personal data is being processed.

Finally, we wish to emphasize that registration is just one of the means to comply with the DPA and related issuances of the NPC. This means that while a company or organization may not be required to register their data processing systems, they are still covered by the other provisions of the DPA, must appoint a DPO, and are mandated to implement reasonable and appropriate security measures to protect personal data they are processing.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[9] See: NPC Advisory No. 2017-03 - GUIDELINES ON PRIVACY IMPACT ASSESSMENTS dated 31 July 2017

ADVISORY OPINION
NO. 2018-20

18 April 2018

[redacted]

Re: POSTING OF THE LIST OF ADMITTED STUDENTS ON THE BULLETIN BOARD OF THE SCHOOL

Dear [redacted],

This refers to your inquiry received by the Privacy Policy Office of the National Privacy Commission (NPC) on 21 March 2018. You asked whether the Data Privacy Act (DPA) of 2012 allows your school to post on its bulletin board, the names of accepted first year medical students in the College of Medicine without the students' consent.

We understand that it has been a common practice among universities such as the University of the East Ramon Magsaysay Memorial Medical Center, Inc. (UERMMMCI), a personal information controller (PIC),[1] to post on its bulletin board, the names of successful applicants to the College of Medicine. This is done without the consent of the students. Under the DPA, such activity is considered as processing[2] of personal information.

The aforesaid publication of the names of admitted applicants is permitted even without the consent of the students, pursuant to Section 12(f) of the DPA, to wit:

> "SECTION 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

---

[1] R.A. No. 10173, §3(h) - Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.

[2] Id., §3(j) - Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."

With regard to how this legitimate interest provision can be used as the appropriate basis for lawful processing, the UK Information Commissioner's Office (ICO) produced a guide on the provisions of the Regulation (EU) 2016/679—which repeals the 1995 EU Directive from which the DPA is based on.

The guide states that legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact.[3]

In order to rely on legitimate interests as basis for lawful processing, the PIC must be able to satisfy its key elements which can be broken down into a three-part test as follows:

1. Purpose test: are you pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interest?

We note that there is a legitimate interest in the posting of the names on the bulletin board of your school, the main purpose of which is to simply inform the applicants that they successfully passed the examinations in the most transparent and practical way.

Likewise, the posting is necessary for the purpose as these applicants are most probably already eagerly waiting for the results of the examinations. It adheres to the principle of proportionality under the DPA because the processing is deemed necessary, adequate, and not excessive in relation to the purpose.

Finally, the balancing test means taking into account if the interests or fundamental rights and freedoms of the data subject do not override the PIC's interests. Recital 47 of the GDPR says:

---

3 Information Commissioner's Office (ICO). (March 22, 2018). Guide on the General Data Protection Regulation (GDPR): Legitimate interests. (available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=34#link10)

> "... At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing...."

Presumably, when an applicant applies for admission, which involves submitting forms with his or her personal information, and subsequently taking the examination, the applicant is aware that the school will process the personal information, particularly his or her name for purposes that are relevant to his or her admission, such as publication of successful applicants' names. This means that the applicant could reasonably expect that his or her name may be posted on the bulletin board of the school if one has successfully hurdled the examinations.

From the foregoing discussions on the legitimate interests provision as the basis for lawful processing, we reiterate that the said posting is permissible under the DPA.

This being said, it is still recommended, in the future, to obtain their consent. For instance, consent may be obtained in their application form for purpose of posting in bulletin boards the names of those accepted. This is a means to ensure that the PIC adheres to principles of transparency and legitimate purpose.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-021

27 April 2018

[redacted]

Re: TELEPHONE DIRECTORIES

Dear [redacted]

This pertains to your initial request for advisory opinion received by the National Privacy Commission (NPC) on 16 November 2017 and your letter response dated 15 March 2018, where we received the additional information and documents in order for us to respond to your initial inquiry.

We understand that you seek to clarify the best approach regarding the residential directory listing of PLDT and its group of affiliates as part of the fulfillment of PLDT's obligations as a telephone service provider vis-à-vis its compliance with Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances of the National Privacy Commission (NPC).

We understand further that PLDT raised the issue of the printing of customer information (name, address, and telephone number) via the Directory Listing and the need for the consent of these customers. PLDT claims that its "base of customers whose details have been printed have not expressly provided their consent to print their details in the existing DPC White Pages that meet the standards of a valid consent as contemplated by the DPA and DPA IRR."

The above concern is specifically true for subscribers acquired prior to July 2017, which is the commencement of PLDT's consent program.

---

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

Telephone Directory

Commonwealth Act No. 146,[3] otherwise known as the Public Service Act, which has been amended by Commonwealth Act No. 454[4] provides for the regulation of public services, specifically wire and wireless communication.

This covers both private entities as well as those owned or operated by government entities or government-owned or controlled corporations.[5] Revised Order No. 1 or the Public Service Commission Rules and Regulations for all Public Services was further enacted to implement the Public Service Act.

Section 149 of Revised Order No. 1 clearly mandates each telephone public service to issue a listing directory at least once a year, to wit:

> "**Telephone Directory.** – Each telephone public service shall at least once a year issue a listing directory showing therein the names of all subscribers arranged in alphabetical order, their addresses and telephone numbers and such other information as may be of interest to a subscriber's every day use of his telephone. Each subscriber shall be entitled to a free copy of the directory."

In relation to such directive, the NTC issued Memorandum Circular No. 05-06-2007[6] (NTC MC) dated 08 June 2007, stating that the consumers or subscribers of telecommunication operators shall be given the option not to be listed in the publication:

> "**Section 2.2**- Any data supplied by the consumer shall be treated as confidential by the entity or service provider mentioned under Section 1.1 hereof and shall not be used for purposes not authorized by him. Upon subscription, he shall be informed of his right to privacy and the manner by which his data would be protected. In cases where a public directory listing of subscribers is regularly published by the service provider, the consumer shall be given the option not to be listed in succeeding publications."

Based on the provision above, subscribers have the right to decide whether they want their name, address and telephone number to be listed and included in the directory for publication.

---

[3] THE PUBLIC SERVICE LAW, "Public Service Act" (07 November 1936).
[4] AN ACT TO AMEND VARIOUS SECTIONS OF COMMONWEALTH ACT NUMBERED ONE HUNDRED AND FORTY SIX, OTHERWISE KNOWN AS THE PUBLIC SERVICE ACT (08 June 1939).
[5] Id., §13.
[6] Consumer Protection Guidelines

Since the NTC issued such circular in 2007, telephone operators are expected to have implemented a procedure or mechanism to inquire whether a consumer or subscriber has elected to be included in the list or not.

Consent

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 his or her personal, sensitive personal, or privileged information.

Indeed, the NTC MC is in consonance with the DPA, whereby the data subjects, or subscribers in this case, has the option to be included or excluded from the list, considering that it involves the publication of personal data of all subscribers in the Philippines.[7]

The NPC recommends the strict implementation of said NTC MC, specifically the provision concerning the need to obtain the consent of the subscriber.

With this, all subscribers who did not provide their consent to be included in the public directory listing should be duly excluded from the same.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[7] Supra note 1, §16.

ADVISORY OPINION
NO. 2018-22

30 April 2018

[redacted]

Re: SCOPE AND COVERAGE OF THE DATA PRIVACY ACT

Dear [redacted],

This refers to your request for advisory opinion received by the National Privacy Commission (NPC) on 16 April 2018, which sought to clarify the coverage and applicability of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA)[1], its Implementing Rules and Regulations (IRR)[2] and relevant issuances. Specifically, you have inquired about the following:

1. Applicability of the DPA to all private employers operating in the Philippines with respect to the personal data of their employees, regardless of the number of the employees;
2. Inclusion of records of past employees in determining the threshold of processing sensitive personal information of at least one thousand (1,000) individuals;
3. Compliance of the organization with the other provisions of the DPA even though the employer is not required to register its personal data processing system; and
4. Applicability of the DPA to a BPO company that processes personal data of data subjects based in the United States.

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

Scope of the DPA

The DPA applies to any natural and juridical person involved in the personal information in the personal information[3] including those personal information controllers (PICs)[4] and processors (PIPs)[5] who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office of agency in the Philippines.[6]

Thus, the DPA shall apply to any private or government entity regardless of the number of employees, as long as they are processing personal data in the Philippines. The number of employees is only material in determining whether the organization is required to register their data processing systems.[7]

The provisions under the Act, IRR, and other relevant orders issued by the NPC must be complied with by the PICs and PIPs, whether they meet the prescribed threshold set by the NPC for registration or not.

Registration of the Data Processing System

The DPA and its IRR requires the registration of the personal data processing systems of PICs and PIPs under any of conditions set by the NPC in Circular 2017-01.[8]

One of the conditions provided for by the issuance is processing which includes sensitive personal information of at least one thousand (1,000) individuals.[9] This threshold pertains to sensitive personal information not just of the employees of the organization but also includes its customers or clients, current or past.

It is important to remember that storage of personal data is considered as a processing activity.[10] Hence, if combined and it reaches one thousand (1,000) individuals, registration is mandatory.

---

[3] Supra note 1, §3(g).
[4] Id., §3(h).
[5] Id, §3(i).
[6] Id., §4.
[7] NPC Circular 17-01: REGISTRATION OF DATA PROCESSING SYSTEMS AND NOTIFICATIONS REGARDING AUTOMATED DECISION-MAKING (31 July 2017), §5.
[8] Id.
[9] Id.,
[10] Supra note 1, §3(j).

Data subjects outside of the Philippines

Section 4 of the IRR clearly states that the DPA and its rules and issuances apply to entities involved in the processing of personal data that are found established or in the Philippines and when such processing is done in the country. Accordingly, the nationality and/or residence of the data subjects are immaterial in this scenario. The BPO company in the Philippines is required to comply with the law.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-024

4 May 2018

[redacted]

Re: REPORTING OF ALLEGED CRIMINALS' PERSONAL DATA

Dear [redacted]

This has reference to your inquiry received by the National Privacy Commission (NPC) via e-mail. You asked how the Data Privacy Act (DPA) of 2012 and its Implementing Rules and Regulations (IRR) affect the practice of some security agencies or establishments of reporting to the Philippine National Police (PNP) and barangay officials, criminal elements who are caught within their premises. You likewise asked if the disclosure of personal information of the alleged suspect such as his/her name, photo, or address, for apprehension purposes, as well as posting of the same in public places, would constitute a violation of the DPA.

Reporting to the police and other law enforcement agencies in relation to a criminal investigation

The practice of security agencies and establishments of reporting to the PNP or barangay officials criminal incidents which happened within their premises and personal information on an alleged criminal offender (data subject[1]), do not constitute a violation of Republic Act (R.A.) No. 10173, otherwise known as the Data Privacy Act (DPA) of 2012.

The processing[2] of personal information of a possible suspect, by reporting to police officers and/or barangay officials of proper jurisdiction, is allowed under Section 12(e) of R.A. No. 10173, specifically the following provision:

[1] R.A. No. 10173, §3(c) - Data subject refers to an individual whose personal information is processed.
[2] Id., §3(j) - Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

> "(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;"

Further, Section 13(f) of the DPA relating to lawful processing of sensitive personal information states that:

> "(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority."

In reporting cases to law enforcement authorities, certain personal information[3] about the suspected perpetrator of the crime will be divulged. This may include names and photographs. This is necessary in order for the police officers to determine and verify the facts of a case, and to aid in their investigation.

In the same manner, police officers' act of gathering data is allowed in accordance with Section 24 of the Republic Act No. 6975[4], which states that the powers and functions of the PNP include, among others, to:

1. Enforce all laws and ordinances relative to the protection of lives and properties;
2. Maintain peace and order and take all necessary steps to ensure public safety;
3. Investigate and prevent crimes, effect the arrest of criminal offenders, bring offenders to justice and assist in their prosecution; and
4. Exercise the general powers to make arrest, search and seizure in accordance with the Constitution and pertinent laws.

Thus, the disclosure of personal information of suspected criminals to law enforcement officers is allowed under the DPA when it is in pursuant to its mandate to investigate and prevent crimes.

---

[3] Id., §3(g) - 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.
[4] AN ACT ESTABLISHING THE PHILIPPINE NATIONAL POLICE UNDER A REORGANIZED DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT, AND FOR OTHER PURPOSES

Investigation refers to the collection of facts to accomplish a three-fold aim: a. to identify the suspect; b. to locate the suspect; and c. to provide evidence of his guilt. In the performance of his duties, the investigator must seek to establish the six (6) cardinal points of investigation, namely: what specific offense has been committed; how the offense was committed; who committed it; where the offense was committed; when it was committed; and why it was committed. Taking of sworn statements of suspects and witnesses is also part of the investigation protocol.

To emphasize this further, while the DPA aims to protect personal and sensitive personal information in information and communications systems in both the government and the private sector, it should not be construed to be limiting the powers and functions of government instrumentalities, especially the law enforcement, in terms of fulfilling their mandate to promote peace and order and ensure public safety for the country.

Posting of name and photo relating to suspects of a crime in public places

General considerations on the posting of personal data of suspects in public places should include the balancing of the rights of the data subject vis-à-vis those of the general public.[5] According to the DPA, the processing of personal information shall only be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.[6]

The public posting of personal information may be allowed in certain instances, i.e. wanted suspects, those who escaped custody, etc.[7] Note that other means of tracing the location of the person should have first been tried where practical.[8]

We note also the common practice of some establishments of posting photos of suspected shoplifters. The Office of Personal Data Protection

[5] Association of Chief Police Officer of England, Wales & Northern Ireland, GUIDANCE ON THE RELEASE OF IMAGES OF SUSPECTS AND DEFENDANTS, May 2009, available at http://library.college.police.uk/docs/acpo/ACPO-Guidance-Release-Images-Suspects-Media.pdf
[6] RA No. 10173, §11.
[7] Supra note 5.
[8] Id.
[9] Greenleaf, Graham. Asian Data Privacy Laws: Trade and Human Rights Perspectives. 2014.
[10] Id.
[11] See: R.A. No. 10173, §12-13.
[12] See: R.A. No. 10173, §16-19; Implementing Rules and Regulations (IRR) of R.A. No. 10173, §34-37.

(OPDP) in Macau have demanded that the same be stopped, reasoning that although it is legal for establishments to install surveillance systems in their premises for security purposes, the image data derived therefrom may not be processed or used for something other than said security purpose. This would exclude the public posting of images of suspected shoplifters and labelling them as such.[9] If video data indicates shoplifting, it should have been referred to the police.[10]

In the Philippines, the use of surveillance systems is likewise considered processing of personal data, and must therefore comply with the requirements of the DPA. These surveillance mechanisms are commonly utilized by establishments for legitimate security purposes, and may have proper basis for lawful processing under the DPA[11] which do not require consent of the data subjects.

However, based on the given circumstances, those establishments engaged in public announcements of an alleged suspect's personal information, are processing in a manner that is unauthorized by the DPA. Such public disclosure of personal data, in particular the alleged suspect's photo, whether derived from the establishment's surveillance footages or acquired elsewhere, may constitute a violation of the provisions of the same law (e.g., rights of the data subjects[12]).

In addition, any processing of personal information must be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.[13] We emphasize that such activity already deviates from the original purpose which is to ensure that the premises are secured and protected. By publicly posting the information of a possible suspect, the purpose becomes an intentional association of the person to the crime for the public's scrutiny, instead of leaving the matter to the police.

Furthermore, the said posting violates the principle of proportionality for being an unnecessary and excessive processing of personal data.[14] Processing could only be allowed if there are no other means to fulfill a legitimate purpose, which is clearly not the case.[15]

---

[9] Greenleaf, Graham. Asian Data Privacy Laws: Trade and Human Rights Perspectives. 2014.
[10] Id.
[11] See: R.A. No. 10173, §12-13.
[12] See: R.A. No. 10173, §16-19; Implementing Rules and Regulations (IRR) of R.A. No. 10173, §34-37.
[13] IRR of R.A. No. 10173, §18(b).
[14] Id., §18(c).
[15] Ibid.

These establishments, as personal information controllers (PIC)[16], are also obliged by the DPA to implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.[17]

Ultimately, in any processing of personal data, it is reminded that PICs give due respect to the fundamental rights, and freedoms of the data subjects which require protection under the Philippine Constitution.

The opinion provided herein is based on the limited information provided and is not intended to address other issues which are not subject of the inquiry.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[16] R.A. No. 10173, §3(h) - Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.
[17] See: R.A. No. 10173, §20; IRR of R.A. No. 10173, §25-29.

ADVISORY OPINION
NO. 2018-25

4 May 2018

[redacted]

RE: REQUEST FOR INFORMATION FROM LAW ENFORCEMENT AGENCIES

Dear [redacted],

This pertains to your request for advisory opinion received by the Privacy Policy Office of the National Privacy Commission (NPC) on 10 April 2018, which sought to clarify whether the disclosure of Cebu Pacific passengers' personal information and travel records to law enforcement agencies is in accordance with Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances of the NPC.

You mentioned in your letter that the Philippine Drug Enforcement Agency (PDEA) filed an administrative case against its employee, [redacted]. In relation to the said case, PDEA would like to confirm [redacted] whereabouts on 16 August 2015. Said personnel presented, as part of his defense the following:

- System generated Cebu Air, Inc. Official Receipt No. [redacted] dated [redacted]' for Php1,734.68; and
- Printout of the online booking with Booking Reference Number [redacted] for [redacted] Cebu to Butuan [redacted].

PDEA requested Cebu Pacific to verify if indeed [redacted] booked a flight and purchased tickets, and if he actually boarded any flights on [redacted] and the time and destination of said travel.

---

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).

Scope of the DPA

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[3] Personal information pertains to any information 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.[4]

Consequently, the name of the passenger is considered as personal information, combined with the flight details, such information taken together will directly and certainly identify the individual.

However, the DPA exempts from its scope information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

1. The fact that the individual is or was an officer of employee of the government institution;
2. The title, business address and office telephone number of the individual;
3. The classification, salary range and responsibilities of the position held by the individual; and
4. The name of the individual on a document prepared by the individual in the course of employment with the government.[5]

Thus, if the personal information being requested relates to an official trip of [redacted], for him to perform his responsibilities as [redacted], supported by an official document from the agency authorizing his trip, his flight details and confirmation on whether he boarded the aircraft are outside the coverage of the DPA.

In fact, this validation is also necessary for accounting and auditing purposes of the government agency, as well as for public information considering the use of public funds.

In the event, however, that the trip of [redacted] is personal in nature, and in no way related to the discharge of his functions in PDEA, the personal information requested is not exempt from the coverage of the law, and Cebu Pacific has the responsibility, as a personal information

[3] Supra note 1, §4.
[4] Id., §3(g).
[5] Supra note 3.

controller, to protect it against unauthorized processing[6] or unauthorized disclosure.[7]

Lawful Processing of Personal Information

Section 12 of the DPA provides that personal information can only be processed if the data subject has given his or her consent, or when processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by third parties to whom the data is disclosed, among other conditions provided by law.

We understand that this certification from Cebu Pacific is a crucial evidence that can incriminate or absolve [redacted] from the ongoing administrative case. It is then considered as a legitimate interest of PDEA, the third party to whom data will be disclosed.

Nevertheless, the PDEA may opt to simply require [redacted]' to personally obtain the certification from Cebu Pacific, seeing that this will greatly strengthen his defense and support his case, otherwise, for [redacted] to authorize PDEA to acquire the certification in his behalf.

This advisory opinion is based on the limited information provided in the request, and may vary based on additional information or when the facts are changed or elaborated.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[6] Supra note 1, §25.
[7] Id., §32.

ADVISORY OPINION
NO. 2018-026

4 May 2018

[redacted]

[redacted]

[redacted]

RE: LAWFUL PROCESSING OF PERSONAL DATA

Dear [redacted]

This is with reference to your request for advisory opinion which sought clarification on whether the processing of personal data by the Capital Markets Integrity Corporation (CMIC) is allowed under Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances of the National Privacy Commission (NPC).

We understand that CMIC is a wholly-owned subsidiary of the Philippine Stock Exchange, Inc. It was granted by the Securities and Exchange Commission (SEC) its self-regulatory organization (SRO) status on 3 February 2012.[3]

We understand further that an SRO refers to an organized exchange, registered clearing agency, organization or association registered as an SRO under Section 39 of the Securities Regulation Code (SRC), and which has been authorized by the SEC to: (1) enforce compliance with relevant provisions of the Code and rules and regulations adopted thereunder; (2)

[1] 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" (15 August 2012).
[2] Implementing Rules and Regulations of the Data Privacy Act (24 August 2016).
[3] Capital Markets Integrity Corporation. About Us. Available at http://www.cmic.com.ph/main/aboutUs.html (last accessed: 4 May 2018)

promulgate and enforce its own rules which have been approved by the Commission, by their members and/or participants, and; (3) enforce fair, ethical and efficient practices in the securities and commodity futures industries including securities and commodities exchanges.[4]

Considering the above, we confirm that CMIC may process personal, sensitive personal and privileged information of data subjects, taking into consideration the provisions of Sections 12 and 13 of the DPA on the criteria for lawful processing of personal data.

Specifically, Section 12 (c) of the DPA provides that processing of personal information shall be permitted when the processing is necessary for compliance with a legal obligation to which the personal information controller is subject. Similarly, for sensitive personal and privileged information, Section 13(b) of the DPA provides that the same may be lawfully processed when processing is provided for by existing laws and regulations: provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data.

We wish to emphasize that the DPA, its IRR and related issuances of the NPC should be read together with existing laws, such as the SRC. The DPA has the twin task of protecting the right to privacy and ensuring the free flow of information. The law cannot be used as an excuse for non-compliance with other existing laws, rules, and regulations.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[4] 2015 IMPLEMENTING RULES AND REGULATIONS OF THE SECURITIES REGULATION CODE (REPUBLIC ACT 8799), Rule 3.1.22.

ADVISORY OPINION
NO. 2018-027

4 May 2018

[redacted]

Re: PASIG CITY ORDINANCE NO. 11 "AN ORDINANCE REQUIRING THE REGISTRATION OF MIGRANTS, TENANTS, BOARDERS AND TRANSIENTS TO THE BARANGAY, AND FOR OTHER PURPOSES"

Dear [redacted]

This pertains to your request for advisory opinion from the National Privacy Commission (NPC) which sought to clarify whether Pasig City Ordinance No. 11[1] (Ordinance) is compliant with Republic Act No. 10173,[2] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and relevant issuances of the NPC, and particularly respond to the following questions:

1. Whether or not the local government of Pasig City is compliant with the DPA vis-à-vis its ability to protect the information they are requesting;
2. Whether or not as a processor, Barangay Kapitolyo is compliant with the DPA; and
3. Whether or not Barangay Kapitolyo has exceeded their authority in requesting for additional information not contemplated by the Ordinance such as birth date, profession and last address, and requesting these from tenants and lessees themselves.

Preliminary to responding to the issues you have presented, it is important to discuss the essence of the Ordinance. It is considered as a local law and is permanent in nature, enacted by the local government unit pursuant to its delegated legislative power.[3] In this case, Ordinance No. 11 was enacted as a preventive measure to minimize the increasing criminal activities within the city and promote peace and order.

[1] Enacted on 15 September 2016.
[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" (15 August 2012).
[3] Municipality of Paranaque vs. V.M Realty Corporation, G.R No. 127820 (20 July 1998).

The Urban Development and Housing Act of 1992 likewise mandates the local government units to set up effective mechanisms to monitor trends in the movement of population, i.e. from rural to urban, urban to urban, and urban to rural areas, and identify measures by which such movements can be influenced to achieve balance between urban capabilities and population, to direct appropriate segments of the population into areas where they can have access to opportunities to improve their lives and to contribute to national growth and recommend proposed legislation to Congress, if necessary.[4]

In Europe, population registers are conducted on a municipal level, which are then consolidated and centralized in a national register, not only for official public purpose but for research and development as well.[5] For other jurisdictions such as Estonia, submission and compilation population registers are part of international obligations for comparison of migration records and facilitation in processing permits.[6]

The highlights of Ordinance No. 11 are as follows:

> **"Section 3. REGISTRATION.** – Owners of dormitories, boarding houses, apartments, bed spaces and rooms are required to submit to their respective barangay offices lists of tenants/lessees, transients and copies of their respective lease agreements within 24 hours upon signing.
>
> Owners who do not execute written contracts should likewise submit the names of their tenants, renters, bedspacers to the barangay office within 24 hours upon start of rental.
>
> **Section 4. ALIEN/FOREIGN LESSEES.** – Owners of dormitories, boarding houses, bedspaces and rooms including warehouses, hotels, inns, apartelles, motels, pension houses whose lessees or actual occupants are aliens of foreign nationals shall submit copies of the contracts and/or lease agreements including copies of passports of aliens or foreign nationals occupying aforesaid properties to the barangay offices having jurisdiction over the property.

---

[4] Republic Act No. 7279, An Act to Provide a Comprehensive and Continuing Urban Development and Housing Program, Establish the Mechanism for its Implementation, and for other purposes, "Urban Development and Housing Act of 1992" (24 March 1992), §37.

[5] Herm, Anne and Poulain, Michel (2013), Central Population Registers as Source of Demographic Statistics in Europe, available at http://www.cairn-int.info/article-E_POPU_1302_0215--central-population-registers-as-a-source.htm

[6] International Migration – Statistical Office of Estonia, available at http://www.stat.ee/dokumendid/19482

Section 5. DUTY OF PERMANENT RESIDENTS WITH VISITORS. – It shall be the duty of every permanent resident who has accepted transients/visitors whose stay shall be for a period of one week or more to report the names of their visitors to their respective barangay offices."

A careful reading of the provisions of the Ordinance will reveal that the duty of submitting the list of tenants or lessees and transients falls on the owners. Hence, there is no basis in collecting the names of the tenants directly from the tenants or lessees themselves. In the event that the owners fail to submit the required information, it is the responsibility of the barangay to go after the owners and penalize them for non-compliance with the directives of the Ordinance.

In your letter-request, you mentioned that persons claiming to be personnel or agents deputized by the barangay went to your house, on at least two separate occasions, to distribute forms which have to be filled up by the homeowners.

The form asks for the following information:

- name of owner;
- address;
- number of units;
- contact details (landline, mobile number and email); and
- type of unit.

Further, the tenants were asked for the following:

- name;
- birthday;
- profession;
- last address;
- address; and
- date of arrival.

First, the Ordinance merely required for the disclosure of the name of the tenant/lessee or transient and for the copy of the lease agreement. Nowhere in the ordinance will require the disclosure of the contact details, birthday, profession, and last address of the tenants.

Second, the deputized members or agents of the barangay must have presented their authority to collect information, as well as the actual copy of the Ordinance and further issuances to support the collection of information. As mentioned above, the tenants are not the one responsible to furnish such information to the barangay, but the owners themselves.

The DPA mandates natural and juridical persons involved in personal information[7] processing[8] to abide by the data privacy principles, uphold the rights of the data subject, and implement security measures in order to protect personal information in their custody.

At the onset, the subject Ordinance must be evaluated in terms of its observance with the data privacy principles.

First, the principle of transparency states that the data subject must be aware of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, and the rights of the data subjects and how these can be exercised.[9] Although the data subject, the constituents, are aware of the nature and purpose of the processing, for public safety and welfare, they were not informed as to the risks and safeguards involved and their rights as data subjects.

Second, the principle of legitimate purpose is clearly provided for in the ordinance, given that the processing of personal information is compatible with the mandate of cities and barangays to enact measures on how to protect its territorial jurisdiction and maintain peace and order.[10]

Lastly, the principle of proportionality states that the processing of information shall be adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose.[11]

Pursuant to the Ordinance, the disclosure of the name and lease agreement with tenants complies with the principle of proportionality. However, the additional information being collected by the alleged agents of the barangay have no basis. There is no necessity for collecting the contact numbers, birthday, profession, and last address of the tenants in relation to the main purpose of the ordinance, which is to maintain a registry or list of owners engaged in the business of leasing real property within its jurisdiction. Thus, with regard to information not required by the ordinance to be disclosed, such information violates the principle of proportionality.

---

[7] Supra note 2., §3(g) 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 identity an individual.
[8] Id., §3(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
[9] IRR, §18(a).
[10] Id., §18(b).
[11] Id., §18(c).

An ordinance enjoys the presumption of validity, and can only be nullified in a direct action assailing its validity or constitutionality.[12] In determining the legality of an ordinance, both the formal (i.e, whether the ordinance was enacted within the corporate powers of the LGU and whether it was passed in accordance with the procedure prescribed by law), and substantive (i.e, involving inherent merit, like the conformity of the ordinance with the limitation under the Constitution and the statutes, as well as with the requirements of fairness and reason, and its consistency with public policy) tests must be satisfied.[13]

In view of the foregoing, Ordinance No. 11 is valid and enforceable. Considering that Barangay Kapitolyo is duty bound to turn over and submit, on a monthly basis, to the City Management Information System (MIS) the list of owners engaged in the business of leasing real property, Barangay Kapitolyo is a considered the personal information processor (PIP)[14], directed by the City Management Information System to process personal information of tenants/lessees and transients, including the collection, organization and consolidation of such personal information, within their barangay.

As a PIP, the barangay is then required to comply with the obligations of a PIP stated in the DPA, its IRR and related issuances, i.e. the duty to implement security measures and uphold the rights of the data subjects, among others.

This advisory opinion is based on the limited information provided in the request, and may vary based on additional information or when the facts are changed or elaborated.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

---

[12] Social Justice Society, et al. vs. Hon. Jose L. Atienza, Jr., G.R No. 156052 (13 February 2008).
[13] Valentino L. Legaspi vs. City of Cebu, T.C (Tito) Sayson and Ricardo Hapitan, G.R No. 159110 (10 December 2013) and Bienenido Jaban, Sr. et. al., vs. Court of Appeals, et. al., G.R o. 159692 (10 December 2013).
[14] Supra note 2., §3(i) Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

ADVISORY OPINION
NO. 2018-028

16 May 2018

[redacted]

Re: OWNERSHIP OF 201 FILES

Dear [redacted]

This pertains to your query received by the National Privacy Commission (NPC) via email. As stated in your email, your wife ("Employee A") requested for her 201 file from her company but was only able to obtain the 201 file from another officemate. Employee A was later reprimanded by the company for serious misconduct by reason of her alleged covert acquisition of the 201 file. You therefore sought clarification on the ownership of an employee's 201 file in a private company.

An employee 201 file, usually containing records pertaining to the employee's personal information, employment contract, duties, salary, performance and employment history, among others, is established and maintained by an employer for specific purposes relating to the employee's employment, i.e. payroll, training and development, performance evaluation, promotion, etc. As this file is compiled and in part, created by and held under the custody of the company, such files may be considered company property and acquiring a copy thereof may still be governed by certain company rules and regulations.

On the other hand, Republic Act No. 10173[1], also known as the Data Privacy Act of 2012 (DPA), applies to the processing[2] of all types of personal information and to any natural and juridical person involved in the processing thereof.[3] Thus, companies that process personal

[1] 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" (15 August 2012).

[2] Id., §4 - Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

information of an individual must comply with the provisions of the DPA.

They are bound to uphold the rights of data subjects,[4] adhere to general data privacy principles of transparency, legitimate purpose and proportionality, and the requirements of lawful processing. They must ensure that data subjects are aware of the nature, purpose, and extent of the processing of their personal data, including the risks and safeguards involved, the identity of personal information controller, their rights as a data subject, and how these may be exercised. Furthermore, they must also provide easy access to information and communication relating to the processing of personal data.[5]

Section 16(c) of the DPA sets forth the data subject's right to reasonable access, upon demand, to the following:

1. Contents of his or her personal data that were processed;
2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the personal information controller.

Accordingly, Employee A, being a data subject, is entitled to have reasonable access to the personal information in her 201 file. She may exercise her right to access in the manner provided under the DPA but she must still abide by company protocols in accessing her 201 file.

Under the law, the company is obligated to respond and grant reasonable access to subject request. Should the request be ignored or denied, a complaint with the NPC may be initiated following the procedure laid down in NPC Circular No. 2016-04, as one of NPC's functions is to enforce and effectively implement the provisions of the DPA, including those pertaining to the rights of data subjects.

---

[3] Id., §4.
[4] Id., §3(c) - Data subject refers to an individual whose personal information is processed.
[5] IRR of RA No. 10173, §18(a).

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-29

6 June 2018

[redacted]

RE: PSEUDONYMIZATION OF PERSONAL AND SENSITIVE PERSONAL INFORMATION

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) on 25 April 2018 for a clarification on pseudonymization and the request of brokers for information.

You mentioned in your email that brokers are requesting detailed utilization reports that contain personal and sensitive personal information of policyholders from health maintenance organizations (HMOs) with pseudonymized personal information as a workaround to the statutory requirement of securing consent from the individuals.

Lawful processing of personal data

We understand that utilization reports contain sensitive personal information, particularly health information, of policyholders. It is important to establish that these personal data entail a higher degree of protection due to the higher risks involved in its processing.

As a general rule, disclosure of sensitive personal information to third parties, such as brokers, is prohibited, unless such processing satisfies any of the conditions set forth in Section 13 of the DPA:

a. The data subject has given his or her consent;
b. The processing is provided for by existing laws and regulations;
c. The processing is necessary to protect the life and health of the data subject or another person;

d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations;

e. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution; or

f. The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

Absent any of the instances enumerated above, disclosure of sensitive personal information to the brokers has no lawful basis.

Pseudonymized personal data

Pseudonymization has been defined as "the processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[1]

It consists of replacing one attribute (typically a unique attribute) in a record by another.[2] The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymization when used alone will not result in an anonymous dataset.[3] The application of pseudonymization is a practical method of securing personal data since it reduces the association between a new dataset and the original dataset, which then decreases the risk of identification.[4]

But note that pseudonymization of personal data does not change the nature of the data – it remains to be personal data.

Thus, the HMOs and the brokers processing pseudonymized personal data are considered as personal information controllers which must have a basis for lawful processing under Sections 12 and 13 of the DPA, respectively. They must adhere to the general data privacy principles,

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [EU GENERAL DATA PROTECTION REGULATION], Article 4(5) (2016)

[2] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed June 5, 2018)

[3] Id.

[4] GDPR Report, Data masking: anonymization or pseudonymization?, available at https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/ (last accessed June 5, 2018.)

implement reasonable and appropriate organizational, physical and technical security measures for the protection of personal data, and must at all times, uphold data subjects' rights.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-030

31 July 2018

[redacted]

RE: REQUEST FOR COMELEC TO COLLECT AND PUBLISH DATA ON WOMEN AND DIFFERENTLY-GENDERED CANDIDATES AND ELECTED OFFICIALS

Dear [redacted]

We write in response to your letter to the National Privacy Commission (NPC) which sought to clarify whether the collection of information regarding candidates' sexual orientation and gender identity and expression (SOGIE) by the Commission on Elections (COMELEC), to be anchored on the provisions of Republic Act No. 9710, known as the Magna Carta of Women, and the publication of the statistics relating thereto, is in accordance with Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA).

This is in relation to the 13 February 2018 letter from the Secretary General of the National Citizens' Movement for Free Elections (NAMFREL), which requested the COMELEC to collect data on the number of women and other differently-gendered individual candidates and eventually elected, for each barangay, disaggregated by the type of election, and to publicize such information, for a better understanding of the political and electoral environment around these two elections.

However, we understand that the Omnibus Election Code[2] does not require the candidates to declare their SOGIE in their Certificates of Candidacy (COC). Hence, your office opined that the collection and publication of gender statistics and sex-disaggregated data of candidates may find legal basis in Section 36(c) of the Magna Carta of Women,[3] to wit:

---

[1] 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).
[2] Omnibus Election Code of the Philippines, Batas Pambansa Bilang 881, § 74 (1985).

> "Section 36. Gender Mainstreaming as a Strategy for Implementing the Magna Carta of Women.
>
> xxx xxx xxx
>
> (c) Generation and Maintenance of GAD Database. All departments, including their attached agencies, offices, bureaus, state universities and colleges, government-owned and -controlled corporations, local government units, and other government instrumentalities shall develop and maintain a GAD database containing gender statistics and sex disaggregated data that have been systematically gathered, regularly updated; and subjected to gender analysis for planning, programming, and policy formulation."

But you likewise stated that your office is not completely convinced that the above statutory provision may be used as basis for the collection and processing of SOGIE of candidates and elected officials.

The Magna Carta of Women recognizes the role and importance of women in nation building and declares that the State endeavors to develop plans, policies, programs, measures, and mechanisms to address discrimination and inequality in the economic, political, social, and cultural life of women and men.[4]

We understand that the current form of the COC has a field for "Gender" and tickboxes for "Male" and "Female". Based on discussions with the COMELEC representatives, these were included on the basis of COMELEC's gender and development (GAD) program.

Be that as it may, we would like to raise several concerns on the collection of candidate's and elected official's SOGIE:

- It is not a requirement under the Omnibus Election Code. Neither is it a qualification for running for public office.
- Collecting such information through the COC may create the belief that it is mandatorily required by law, and thus, may cause a level of compulsion on the part of candidates to provide an answer which they may not be comfortable to share to the public.
- There is uncertainty as to how such data will be actually

[3] An Act Providing for the Magna Carta of Women [THE MAGNA CARTA OF WOMEN], Republic Act No. 9710 (2009).
[4] The Magna Carta of Women, § 2.

collected through the COC form, i.e., a tick box for "Others" or a blank where candidates may indicate an open-ended response, etc. This may be construed as gender insensitive. Also, the COMELEC may have a difficult time analyzing data from open-ended responses.

- Even if COMELEC will only publish statistics and aggregated data relating to the SOGIE collected, it is still possible for copies of the COCs to be released to the public through Freedom of Information (FOI) requests and to third parties when there are disqualification cases.

From the foregoing, we caution against the collection of SOGIE through official COMELEC forms such as the COC as the same is not absolutely necessary for COMELEC's mandate and for the overall electoral process in the country.

COMELEC and/or NAMFREL may explore other avenues for collecting such information if they still wish to do so, i.e., voluntary surveys.

Collection and processing of sensitive personal information

If and when SOGIE of candidates and elected officials is collected, we emphasize that the processing thereof should always adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

COMELEC and/or NAMFREL must be able to explain to the data subjects the nature, purpose, and extent of the processing of his or her personal data. The processing must be limited to the declared and specified purpose, i.e., gender analysis for planning, programming, and policy formulation for a better understanding of the political and electoral environment of elections. And lastly, processing of the SOGIE information should be adequate, relevant, suitable, necessary, and not excessive in relation to the purpose.

As a personal information controller, COMELEC should uphold data subjects' rights, and implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal data, taking into consideration that SOGIE is sensitive personal information.
This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-031

20 July 2018

[redacted]

Re: PRIVACY NOTICE

Dear [redacted],

This is in response to your request for review of Metro Antipolo Hospital's draft Notice of Privacy – Acceptance of Terms and Conditions of the Privacy Notice and Consent to Use of your Personal Health Information, taking into consideration the requirements of Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulation (IRR), and issuances of the National Privacy Commission (NPC).

Privacy Notice vs. Consent

At the outset, it must be clarified that the submitted privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[2] A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.[3]

Having stated that, there is also a need to determine and clarify the distinction between privacy notice and securing the consent of the data subject for the processing of his or her personal information.
Being a mere notice, it is emphasized that the privacy notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects.

---

[1] 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).
[2] IAPP, Glossary of Privacy Terms, available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2
[3] Id.

The principle of transparency mandated by the DPA dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[4] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[5]

Thus, in line with the right to information of the data subject, personal information controllers (PICs) are required to apprise the data subject of the following:

1. Description of the personal data to be processed;
2. Purposes for processing, including: direct marketing, profiling, or historical, statistical or scientific purpose;
3. Basis of processing, when processing is not based on the consent;
4. Scope and method of processing;
5. Recipient/classes of recipients to whom the personal data are or may be disclosed;
6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
7. Identity and contact details of the PIC or its representative;
8. Retention period; and
9. Existence of rights as data subjects, the right to lodge a complaint before the NPC.

On the other hand, obtaining consent from the data subject for the purposes of processing his or her personal data is a different requirement altogether.

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 his or her personal, sensitive personal, or privileged information.

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic or recorded means.[6]

---

[4] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(a) (2016).
[5] Id.
[6] RA No. 10173, §3(b).

From the foregoing, the following are our observations for your consideration:

Metro Antipolo Hospital and Medical Center, Inc. Privacy Notice	Remarks
USES AND DISCLOSURE OF YOUR HEALTH CARE INFORMATION: • Treatment • Payment • Health Care Operations • Personal Representatives • Family and Friends • Public Health and Safety • Legal Actions De-Identified Health Information Incidental Disclosures	There is a need to define or describe health care information. Further, it is also necessary to determine what health care information will be used and disclosed for each enumerated item. Also, kindly expound further on each item by providing a discussion on specific purpose/s, basis of processing, scope and method of processing, storage, etc.

Metro Antipolo Hospital and Medical Center, Inc. Privacy Notice	Remarks
NOT REQUIRED WRITTEN AUTHORIZATION: • Treatment • Payment • Health Care Operations • Required by Law • Threat to Health or Safety • Abuse or Neglect • Communicable Diseases • Public Health Activities • Medical Research	Kindly clarify the statement "Not Required Written Authorization." We understand that there are processing of sensitive personal information which may not require consent, *i.e.* processing pursuant to laws and regulations. Nonetheless, it is advisable to include a statement to the effect that the hospital will obtain the data subjects' consent at the most opportune time should consent be the appropriate basis for processing.
RETENTION AND DISPOSAL OF HEALTH RECORDS • IN - PATIENT RECORDS - 15 YEARS • OUT – PATIENT RECORDS - 10 YEARS • MEDICO-LEGAL RECORDS - PERMANENT	It may be advisable to indicate the basis, i.e. DOH issuance, law or regulation, hospital policy, etc., of the retention periods.

SIGNATURE OVER PRINTED NAME & DATE ☐ PATIENT ☐ PATIENT REPRESENTATIVE ☐ PATIENT GUARDIAN	To reiterate, a privacy notice is not equivalent to a consent form. Hence, requiring the signature of a patient as part of a privacy notice is not necessary. However, we understand that the hospital may require the signature as part of the documentation that the patient was duly informed regarding the processing of his or her personal data. If this is the case, the same must be clearly stated in the notice in order to avoid any confusion as to what the patient is signing.

It is also advisable to include statements on third party service providers and physician-patient privileged communication.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

ADVISORY OPINION
NO. 2018-032

26 November 2018

[redacted]

Re: PPP CENTER PRIVACY MANUAL

Dear [redacted],

We write in response to your letter request received by the National Privacy Commission (NPC) for the review of the Public-Private Partnership Center's (PPP Center) Privacy Manual in relation to its compliance with the Data Privacy Act of 2012 (DPA)[1] and its Implementing Rules and Regulations (IRR)[2]. A copy of the draft Privacy Manual provided is attached herewith as Annex "A."

Please see comments below on the draft PPP Center Privacy Manual:

PPP Center Privacy Manual	Remarks
Privacy Manual Logo	As the Privacy Manual pertains solely to the PPP Center's privacy policies, kindly remove the NPC seal and retain the PPP seal.
I. Introduction	It should be "Data Privacy Act of 201**2**".
II. Definition of Terms "Data Protection Core Team or DPCT – refers to the team that would assist the Data Privacy Officer…"	DPO pertains to the Data *Protection* Officer.

1 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. IO 173 (20 I 2).
2 Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. IO 173.

III. Scope **Third paragraph**: "... as well as the Personal Data under the control or custody of a private entity that is being shared with or transferred to a Government Agency, shall be protected in compliance with the Act."	Please clarify. Perhaps the intention was to refer to the personal data being with or transferred to the PPP Center shared by a private entity and not just any other Government Agency. In that case, the inclusion of such in the scope is accurate since the personal data will then be under the custody of the PPP Center thus calling for the application of the Privacy Manual.
Fourth paragraph: "The Center may use this Privacy Manual to issue and implement more detailed policies and procedures, which reflect its specific operating requirements."	We suggest to include the term "technical": "The Center may use this Privacy Manual to issue and implement more detailed policies and procedures, which reflect its specific **TECHNICAL AND** operating requirements."
IV. Processing of Personal Data	As a matter of form, we suggest to remove the examples in the parentheses for the subsections as it was merely for drafting guidance.
A. Collection	Please clarify as it seems that based on the current provision, the collection of all personal data will be through the consent form (Annex 1). Note that there will be collection and processing of personal data which is not based on consent, i.e. fulfillment of a contract, processing provided for by existing laws and regulations, among others. Hence, it advisable to provide for the other modes and basis for collecting personal data.
B. Use "Personal Data collected shall be used by the Center for identification, documentation and other legal purposes."	"Other legal purposes" is vague. The DPA mandates that the processing of data shall have a specific and defined purpose. Expound or enumerate the specific uses of the data collected from guests, employees of the PPP Center, etc.
C. Storage, Retention and Destruction "All information gathered shall not be retained for a period longer than one (1) year, unless advised otherwise by the DPO."	Note that there are existing rules and regulations governing the retention period of certain records, i.e. tax purposes, Republic Act No. 9470 (National Archives of the Philippines Act of 2007), etc. Hence, it may be advisable to include a statement that the general rule for the retention period is one (1) year, subject to existing laws, rules and regulations on retention of specific records and documents, and as may be otherwise advised by the DPO in specific instances.

V. Control Framework for Data Protection **B. Physical Measures** **3. Encryption of Personal Data digitally processed** "The CBKMS shall develop a password policy that will be enforced through a system management tool."	Please define what CBKMS is.
B. Physical Measures **8. Retention and disposal procedure**	See comments above on retention.
C. Technical Measures "Each PIC and PIP must implement technical security measures…"	The PIC must pertain to the PPP Center as the PIC in this manual. Thus, it may be rephrased as "The Center shall implement technical security measures…" Should the PPP Center mean that it has PIPs under its control, please specify.
VI. Breach and Security Incidents "Every PIC or PIP must develop and implement policies and procedures…"	Same comment as above.
2. Measures to prevent and minimize occurrence of breach and security incidents "… In particular, the DPO shall monitor the compliance of the Personal Information Processors (PIP) and Personal Information Controllers (PIC) with the DPA."	Same comment as above. Rephrase to: "… the DPO shall monitor the compliance of the Center and its PIPs with the DPA."
5. Documentation and reporting procedure of security incidents or a Personal Data breach "The DPCT shall ensure proper data breach and security incident management by the PIPs and PICs…"	Same comment as above. Rephrase to: "The DPCT shall ensure proper data breach and security incident management by the Center...." Should the PPP Center mean that it has PIPs under its control, please specify so.
VII. Inquiries and Complaints "Every Data Subject has the right to reasonable access to his or her Personal Data being processed by the Personal Information Controller or Personal Information Processor."	Same comment as above. Rephrase to: "Every Data Subject has the right to reasonable access to his or her Personal Data being processed by the Center."

OTHER COMMENTS:

1. Annex 1 – Consent Form

   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.

There is a need to revise this form as consent has to be specific in relation to a particular processing of personal data.

We reiterate that there are lawful processing activities that is not based on consent. Please refer to Sections 12 and 13 of the DPA for the criteria for lawful processing of personal and sensitive personal information.

2. Annex 2 – Inquiry Summary Form

   As stated in the form, it may be submitted via fax, courier or hard copy mail.

   Please note that pursuant to Section 28 of NPC Circular No. 16-01 - Security of Personal Data in Government Agencies, facsimile technology shall not be used for transmitting documents containing personal data. Hence, the PPP Center should consider revising the method of transmitting Annex 2.

   Also, the terms "Data Privacy Officer" and "Data Protection Officer" were used in this form. Please choose the appropriate nomenclature and be consistent in all documentation.

3. Annex 4 – Access and/or Alteration Request Form

   On Section 7 – Disclaimer, please correct the title of the law from Data Protection Act of 2012 to Data Privacy Act of 2012.

4. If you have additional questions or require further clarification, please contact the NPC Privacy Policy Office at 02-510-7836.

For your information.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-033

26 November 2018

[redacted]

Re: DATA SHARING, CONSENT, AND COMPLIANCE WITH THE DATA PRIVACY ACT OF 2012

Dear [redacted],

This is in response to your request received by the National Privacy Commission (NPC) concerning various inquiries and clarifications regarding Republic Act No. 10173,[1] known as the Data Privacy Act of 2012 (DPA), particularly, the following:

1. If two PICs agree to share data with a data sharing agreement signed stating that compliance to the Data Privacy Act will be separate responsibilities, will both PICs be held responsible for a violation committed by only one of them if violation involves the shared data (e.g., non-encryption, processing without consent)?

2. Is there any standard as to how a recipient of personal data will ensure that the data to be received is being shared with consent from the data subject? Is a certification/ contract stating that consent from data subjects were obtained sufficient?

3. Is there a benefit in obtaining new consent via SMS or other means of communication (purpose is processing with another PIC/PIP) if the same data subject has previously signed a consent form for the same purpose? Is there any timeline on the validity of a signed consent if nothing is stated in the consent form? As context to the above, a data partner of the company sends SMS

[1] 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).

opt-in confirmation to potential clients before our company's loan approval. The SMS asks the data subject whether he consents to data partner giving its score to HCPH based on its transaction data with Company A (not the data partner). These data subjects have already signed the HCPH consent form where it states HCPH may collect data from described third-parties.

4. In the context of mobile operators sending SMS messages to its subscribers with direct marketing offers for third party products and services, it is understood that prior consent from the subscribers is required. What practical methods/channels is considered acceptable for obtaining such consent from the existing subscriber base of such mobile operators?

We provide the following clarifications:

Data sharing and compliance with the DPA

To clarify, all personal information controllers (PICs) and personal information processors (PIPs) are mandated to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and issuances of the NPC.

PICs that share personal data under a data sharing agreement (DSA) are mandated to put in place adequate safeguards for data privacy and security in compliance with applicable laws and regulations. The DSA should include a general description of the security measures that will ensure the protection of the personal data of data subjects. The DSA, considering its terms, allows PICs to use contractual and reasonable means to provide safeguards for data protection to the personal data being shared.

Where a PIC fails to put in place the security measures required by law, regulations and the DSA, the said PIC may be solely accountable in the absence of fault or negligence on the other PIC. If no security measures are put in place by both parties or the DSA fails to provide for the same, both parties may be held accountable. Nonetheless, the determination of liability, if any, will be based on the particular facts and circumstances of the case.

Data sharing and consent of the data subject

In relation to data sharing arrangement, the DSA or the pertinent contract may stipulate such fact or guarantee that the PIC sharing the personal

data has collected or processed such on the basis of any of the criteria for lawful processing of personal and sensitive personal information under Sections 12 and 13 of the DPA, and that the data subject consented to the data sharing, unless consent is not required for the lawful processing of personal data.

Consent

Under Section 3(b) of the DPA, consent is defined as 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.

From the definition provided above, it is clear that consent must be evidenced by written, electronic, or recorded means.[2] Any of the three (3) formats provided may be adopted by a PIC. Nonetheless, it is worth emphasizing that, regardless of the format of the consent given by the data subject, it must be freely given, specific, and informed.[3]

In line with the foregoing discussion, implied, implicit or negative consent is not recognized under the law.

Further, as to whether there is a timeline on the validity of a signed consent if nothing is stated in the consent form, the IRR states that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose.[4] The time-bound element does not necessarily mean that a specific date or period of time has to be declared. Thus, for instance, declaring that processing will be carried out for the duration of a contract between the PIC and the data subject may be a valid stipulation.

Also, as long as the purpose, scope, method and extent of the processing remains to be the same as that disclosed to the data subject when consent was given, the consent remains to be valid.

Where applicable, such as in cases where the period of processing can be reasonably ascertained at the time of collection, a PIC may specifically provide for the period of validity of a consent obtained from

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §3(c).
[3] Id.
[4] Id. § 19 (a) (1).

a data subject. The limitation merely emphasizes that consent cannot be overly broad and perpetual for this would undermine the very concept of consent as defined in the law.

We understand that as far as HCPH is concerned, the basis of processing personal data would be the consent of the data subject and/or the contractual relation with the data subject or taking steps at the request of the data subject prior to entering into a contract.

It must be clearly conveyed to the data subject that prior to the loan approval, HCPH would be conducting due diligence and/or further investigation on the applicant-data subject, which will involve collecting further information from third-party sources, and the data subject must consent to the same. Further, these third-party sources must be identified, and the data subject must authorize them to share information with HCPH. Finally, the data subject has to be notified of the transfer of transaction data from Company A to the data partner, the processing done by the data partner and the relationship between the data partner and HCPH, and data subject has to specifically consent and authorize such transfer and processing.

Direct marketing through SMS messages and consent of the data subject

You mentioned that mobile operators would send direct marketing offers for third party products and services via SMS messages to its existing subscriber base. In relation to the same, you inquired on the acceptable practical methods or channels for obtaining consent from the said subscribers.

If consent is the appropriate basis for processing made by the said mobile operators, it is possible for them to obtain consent through an SMS request. For postpaid subscribers, there is an option of sending hardcopy consent forms. Lastly, for those with online accounts with these mobile operators, sending consent forms online through their respective account dashboards or email may also be considered.

The mobile operators should come up with the most efficient and effective way of obtaining consent, taking into consideration the type of processing they will do.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-034

20 July 2018

[redacted]

RE: BUREAU OF INTERNAL REVENUE REQUEST FOR INFORMATION

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) on 13 July 2018 for a clarification on whether the Philippine Medical Association (PMA) may disclose information to the Bureau of Internal Revenue (BIR).

Specifically, the BIR Collection Service through an Access Letter dated 11 July 2018, attached as Annex "A", requested from the PMA a Certification indicating the status of the membership in the PMA of a certain individual. The BIR provided the name and registered address of the said person. In addition, the BIR further requested for the name/s of any entity affiliated to the said person in the conduct of his medical practice to be included in the Certification.

The BIR cited Section 5(B) of the National Internal Revenue Code (Tax Code) as basis for its request for information. Said section provides as follows:

> "SEC. 5. Power of the Commissioner to Obtain Information, and to Summon, Examine, and Take Testimony of Persons. – In ascertaining, the correctness of any return, or in making a return when none has been made, or in determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance the Commissioner is authorized:

> (B) To obtain on a regular basis from any person other than the person whose internal revenue tax liability is subject to audit or investigation, or from any office or officer of the national and local governments, government agencies and instrumentalities, including the Bangko Sentral ng Pilipinas and government-owned or -controlled corporations, any information such as, but not limited to, costs and volume of production, receipts or sales and gross incomes of taxpayers, and the names, addresses, and financial statements of corporations, mutual fund companies, insurance companies, regional operating headquarters of multinational companies, joint accounts, associations, joint ventures or consortia and registered partnerships, and their members: Provided, That the Cooperative Development Authority shall submit to the Bureau a tax incentive report, which shall include information on the income tax, value-added tax, and other tax incentives availed of by cooperatives registered and enjoying incentives under Republic Act No. 6938, as amended: Provided, further, That the information submitted by the Cooperative Development Authority to the Bureau shall be submitted to the Department of Finance and shall be included in the database created under Republic Act No. 10708, otherwise known as 'The Tax Incentives Management and Transparency Act (TIMTA)."

Republic Act No. 10173,[1] known as the Data Privacy Act of 2012 (DPA), provides the criterion for lawful processing of personal information under Section 12(e), i.e. that the processing is necessary in order to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

The Implementing Rules and Regulations (IRR) of the DPA defines a public authority as any government entity created by the Constitution or law and vested with law enforcement or regulatory authority and functions.[2]

The BIR is a public authority. Its powers and duties shall comprehend the assessment and collection of all national internal revenue taxes, fees, and charges, and the enforcement of all forfeitures, penalties, and fines connected therewith, including the execution of judgments in all cases

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3(r) (2016).

decided in its favor by the Court of Tax Appeals and the ordinary courts.[3] The BIR shall give effect to and administer the supervisory and police powers conferred to it by the Tax Code or other laws.[4]

Be that as it may, it is incumbent upon the BIR to demonstrate that the information being requested from the PMA is necessary in order to fulfill its function of determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance.[5]

Prior to disclosing the requested information, it is advisable for the PMA to ask and clarify from the BIR the relation of the PMA Certification indicating the status of the membership of a person vis-à-vis the BIR audit or investigation of the tax liabilities, if any, of the said person following the general data privacy principl es of legitimate purpose and proportionality. The BIR Access Letter provided the contact details of the Chief of its Accounts Receivable Monitoring Division (ARMD) for any clarifications on the request.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commission and Chairman

[3] An Act Amending the National Internal Revenue Code, as Amended, and for Other Purposes [TAX REFORM ACT OF 1997], Republic Act No. 8424 (1997)
[4] Id., § 2
[5] Id., § 5

ADVISORY OPINION
NO. 2018-35

20 July 2018

[redacted]

RE: CERTIFIED LIST OF DECEASED PERSONS REQUIRED UNDER REPUBLIC ACT NO. 8189

Dear [redacted]

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) on 10 July 2018 for clarification on the requirement of Republic Act (RA) No. 8189 or the Voter's Registration Act of 1996 for the submission of a certified list of deceased persons by Local Civil Registrars to the COMELEC Election Officer for the purpose of cancelling their voter registration. You asked if providing the said list is violative of the provisions of RA No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA).

Section 29 of RA No. 8189 provides as follows:

> "Section 29. Cancellation of Registration. The Board shall cancel the registration records of those who have died as certified by the Local Civil Registrar. The Local Civil Registrar shall submit each month a certified list of persons who died during the previous month to the Election Officer of the place where the deceased are registered. In the absence of information concerning the place where the deceased is registered, the list shall be sent to the Election Officer of the city or municipality of the deceased's residence as appearing in his death certificate. In any case, the Local Civil Registrar shall furnish a copy of this list to the national central file and the proper provincial file.

[1] 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).

The Election Officer shall post in the bulletin board of his office a list of those persons who died whose registrations were cancelled and furnish copies thereof to the local heads of the political parties, the national central file, and the provincial file."

Compliance with the provisions and requirements of existing laws is not violative of the DPA. In fact, the DPA provides for the criteria for lawful processing of personal information such as compliance with a legal obligation to which the personal information controller is subject[2] and processing which is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.[3]

We wish to emphasize that the DPA, its Implementing Rules and Regulations, and related issuances of the NPC should be read together with existing laws, such as election laws. The DPA has the twin task of protecting the right to privacy and ensuring the free flow of information. The DPA should not be used as an excuse for non-compliance with other existing laws, rules, and regulations.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[2] RA No. 10173, 12(c)
[3] RA No. 10173, 12(e)

ADVISORY OPINION
NO. 2018-36

23 July 2018

[redacted]

RE: DATA SHARING WITH THE MANILA INTERNATIONAL AIRPORT AUTHORITY (MIAA)

Dear [redacted],

We write in response to your letter dated 6 June 2018 requesting for clarification regarding data sharing under Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA). Specifically, you seek to clarify whether air carriers may transfer personal information of ticket holders for the purpose of refunding terminal fees, without securing ticket holders' consent and without executing a data sharing agreement with the Manila International Airport Authority (MIAA).

We understand that since August 2012, members of the Air Carriers Association of the Philippines (ACAP), namely: Air Philippines Corporation (PAL Express), Cebgo, Inc. (Cebgo), Cebu Air, Inc. (Cebu Pacific), Philippine Airlines, Inc. (PAL), and Philippines AirAsia, Inc. (AirAsia), have been collecting terminal fees directly from prospective passengers for their flights from the Ninoy Aquino International Airport.

The carriers then remit the collected terminal fees to the MIAA after the passengers have taken their flights. The carriers submit the following to MIAA:

1. List of flights covered;
2. Number of passengers for each flight; and
3. Amount of terminal fees collected.

[1] 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).

Thus, under the current system, carriers do not provide any perso nal information to the MIAA.

MIAA is currently looking into a possible transfer from the carriers to MIAA of the terminal fees collected, including unused and unrefunded fees, with the intention to refunding the same to the ticket holders unable to take their flights. This proposed system will necessarily entail the transfer of personal information of ticket holders from the carriers to MIAA.

Data Sharing

The Implementing Rules and Regulations (IRR) of the DPA defines data sharing as the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller.[2]

A data sharing agreement (DSA) refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more personal information controllers.[3]

NPC Circular No. 16-02 sets out the guidelines for data sharing and DSAs involving government agencies. The circular covers personal data under the control or custody of a private entity that is being shared with or transferred to a government agency, and vice versa.[4] Furthermore, the issuance states that a DSA is required when personal data is shared or transferred for the purpose of performing a public function or providing of a public service.[5]

As mentioned above, the contemplated transfer of terminal fees collected, including unused and unrefunded fees for refunding the ticket holders, to MIAA, will necessarily entail the transfer of personal data of each ticket holder (i.e., names, birthdates, contact details, bank details, credit card details, flight details, other personal information) to MIAA.

Considering the foregoing, the contemplated transfer of collected fees and personal data from the air carriers to MIAA falls squarely under the meaning of data sharing. Thus, a data sharing agreement is required.

---

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §3(f) (2016).
[3] NPC Circular No. 16-02, §3(E)
[4] Id., §2.
[5] Id., §1.

Subject to the separate determination of whether this proposed transfer of responsibility in refunding terminal fees to the MIAA is operationally feasible, it is recommended that an amendment of the existing Memorandum of Agreement between MIAA and the air carriers regarding the Passenger Service Charge (PSC) be made to include the required contents of a DSA pursuant to NPC Circular No. 16-02, and incorporate the data privacy principles, enforcement of the rights of data subjects, and implementation of appropriate security measures.[6]

Furthermore, it should be noted that bookings of ticket holders prior to the effectivity of the DPA is still covered by the DPA. As we understand, the air carriers still store and retain personal information in relation to the said bookings and transfer thereof is yet to be done. The storage, retention, and transfer thereof are considered processing[7] under the DPA and such processing is still ongoing until the present. As such, the DPA applies.

Consent of ticket holders to the data sharing

NPC Circular No. 16-02 provides that the consent of the data subjects to the data sharing is required except when such consent is not required for lawful processing[8] of personal data.[9]

Section 5 of Executive Order No. 903[10] states the following powers and functions of MIAA, among others:

- To control, supervise, construct, maintain, operate and provide such facilities or services as shall be necessary for the efficient functioning of the Airport;

- To promulgate rules and regulations governing the planning, development, maintenance, operation and improvement of the Airport and to control and/or supervise as may be necessary the construction of any structure or the rendition of any service within the Airport;

- To perform such other acts and transact such other business,

[6] Id., §6.
[7] Republic Act No. 10173, § 3(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
[8] See: Republic Act No. 10173, §12 and 13.
[9] See: NPC Circular No. 16-02, §4.
[10] Executive Order No. 903, Providing for a Revision of Executive Order No. 778 Creating the Manila International Airport Authority, Transferring Existing Assets of the Manila International Airport to the Authority, and Vesting the Authority with Power to Administer and Operate the Manila International Airport (July 21, 1983).
[11] See: Republic Act No. 10173, §16(a).

directly or indirectly necessary, incidental or conducive to the attainment of the purposes and objectives of the Authority, including the adoption of necessary measures to remedy congestion in the airport;

As stated in MIAA Memorandum Circular No. 06, series of 2017, the refund of terminal fees for unused tickets is anchored on the abovementioned powers and functions of MIAA. Thus, the data sharing is considered necessary for compliance with a legal obligation to which the personal information controller is subject and is pursuant to existing laws and regulations. Considering the foregoing, the data sharing agreement may proceed without the need to obtain the consent of ticketholders.

Nevertheless, the ticket holders should be duly informed that their personal information will be shared with the MIAA for purposes of refunding of the terminal fees, pursuant to the right of data subjects to be informed of the processing of their personal information.[11]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[11] See: Republic Act No. 10173, §16(a).

ADVISORY OPINION
NO. 2018-37

8 August 2018

[redacted]

RE: APPLICABILITY OF THE DATA PRIVACY ACT OF 2012 TO PHYSICAL OR ONLINE ARCHIVES AND LIBRARIES

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) regarding the applicability of Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), to physical or online archives and libraries. Particularly, you are inquiring whether the DPA applies to access to archival records which contain information of deceased individuals as well as church records used for historical research.

Scope of the DPA

At the outset, **there is no conflict between the DPA and Republic Act No. 9470[2] or the National Archives of the Philippines Act of 2007 (NAP). It should be noted that the DPA has the twin task of protecting the fundamental human right of privacy and ensuring the free flow of information to promote innovation and growth.[3] Thus, the law will not operate to curtail the applicability of laws and regulations relative to archives and libraries.**

As such, the pertinent provisions of the NAP will primarily apply as to the management and administration of all public records with archival value, held by either government offices or private collections, for the protection of public documents and records for the preservation of the country's cultural heritage and history.

---

[1] 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).
[2] An Act to Strengthen the System of Management and Administration of Archival Records, Establishing for the Purpose the National Archives of the Philippines, and for other Purposes [NATIONAL ARCHIVES OF THE PHILIPPINES ACT OF 2007], Republic Act No. 9470 (2007).
[3] Republic Act No. 10173, §2.

Nevertheless, when libraries and archives process personal information, the DPA will apply. As stated in Section 4 of the DPA, it applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Processing has a very broad definition and includes essentially anything which one can do with personal information, including, but not limited to its collection, storage, use, retrieval, disclosure, and disposal.[4]

In this regard, the DPA, its IRR, and other related issuances of the NPC shall apply to archives and libraries when they use, store and provide access to archival records which contain personal information.

Libraries and archives are then obliged to comply with the provisions of the DPA, its IRR and other NPC issuances that are relevant to their operations and to the nature of information that they are processing. They must adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.[5] Libraries and archives are also mandated to uphold the rights of the data subjects[6] and implement security measures for the protection of personal data.

Processing for historical research purposes

As to historical research, it is important to note that personal information processed for research purposes is outside of the scope of the DPA.[8] The same is reiterated in the IRR, which further states that the Act shall not apply to personal information processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations or ethical standards.[9] This encompasses access to archival records and church records that may contain personal information for historical research.

This exemption, however, applies only to the minimum extent necessary to achieve the specific purpose, function, or activity. Also, this entails the concomitant responsibility of ensuring that appropriate organizational, physical and technical security measures are in place to protect the personal data being processed for historical research purposes.

Although the consent of the data subjects may not be required in certain instances, the person or organization conducting the research

[4] See: Republic Act No. 10173, §3(j).
[5] Republic Act No. 10173, §11.
[6] Id., §16.
[7] Id., §20.
[8] Id., §4(d).
[9] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §5(c) (2016).

must recognize the rights of the data subjects, including the right to be informed, among others.[10] The data subjects must be aware of the nature of the processing activities, the purpose of processing, the retention period of personal data and the enforcement of their rights.[11]

Likewise, Section 11(f) of the DPA provides that personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed, provided that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law, may be stored for longer periods.

We note also that pursuant to the EU General Data Protection Regulation, the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.[12] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is considered to be processing that is lawful and compatible to the original purpose for which such information were collected or processed.[13]

Further, the law does not prescribe a specific retention period, but rather, applies the laws, rules, or regulations pertinent to a specific industry or sector. In the absence of such, retention of personal data shall only be for as long as necessary for the fulfillment of the declared, specified, and legitimate purpose.[14]

These provisions should complement the NAP specifically on provisions applicable to records stored with permanent and enduring archival value. Thus, libraries and archives should strive to strike a balance in order to determine on a case-to-case basis whether access to archival records containing personal information for historical research meets both the requirements of the NAP and those of the DPA.

Deceased individuals

While the DPA does not explicitly provide for its applicability on personal information of deceased individuals, Section 17 thereof specifically

[10] Maldoff, Gabe. How GDPR changes the rules for research, available at https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (last accessed 16 July 2018).
[11] Id.
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [EU GENERAL DATA PROTECTION REGULATION], Recital 50 (2016).
[13] Id.
[14] See: Republic Act No. 10173, §11(e).

grants the lawful heirs and assigns of the data subject the right to invoke the rights of the data subject at any time after death or when the data subject is incapacitated or incapable of exercising his or her rights. Hence, when personal data of deceased individuals are processed, they are still considered as data subjects and the lawful heirs and assigns may exercise the rights of the deceased as a data subject.

Consequently, processing of personal information of deceased individuals requires the concomitant responsibility to observe general data privacy principles of transparency, legitimate purpose, and proportionality, as well as the implementation of appropriate security measures as required by the DPA. Note, however, considering the foregoing discussion on processing for historical research, personal information of deceased individuals processed for research purposes may be exempt from the coverage of the DPA.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-38

30 July 2018

[redacted]

RE: PERSONAL INFORMATION CONTROLLER IN THE PROCESSING OF CONCESSIONARY BEEP™ CARDS

Dear [redacted]

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought to clarify whether the Department of Transportation (DOTr) is considered as the personal information controller (PIC) in the context of data processing for the issuance of Concessionary beep™ Cards.

In your letter, you have mentioned that there is currently a discussion as to who is the PIC and personal information processor (PIP) between the DOTr and AF Payments Inc. (AFPI), the entity tasked to issue the Concessionary beep™ Cards to identified patrons, in compliance with the Automated Fare Collection System (AFCS) Concession Agreement between AFPI and the DOTr.

Republic Act No. 101731, also known as the Data Privacy Act of 2012 (DPA), clearly defines a PIC in Section 3(h) as the person or entity who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.2

---

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3(m) (2016).

On the other hand, a PIP is any natural or juridical person to whom a PIC may outsource the processing of personal data pertaining to a data subject.[3]

Based on the definitions, it is apparent that it is the DOTr, with its mandate to establish and administer comprehensive and integrated programs to improve the transportation system of the country,[4] that has control over the AFCS, and is thereby considered as the PIC.

As described in your letter addressed to [redacted] of AFPI dated [redacted], personal information of the applicants is gathered by the Public Transport Operators (PTOs) then submitted to AFPI for their processing.

Although AFPI directly handles and processes personal information of applicants turned over by the PTO, we understand that such direction was derived from the instructions given by the DOTr. AFPI remains to be the PIP to whom DOTr has outsourced the processing under the AFCS Concession Agreement, notwithstanding the fact that AFPI manages and oversees the system.

It is worthy to note that indeed, while PIPs exercise some degree of control and are given freedom to execute technical strategies to carry out the activities instructed by the PIC, it is still the PIC who exercises overall control over the purpose and manner of processing.[5] Particularly, when the basis of personal data processing is the statutory mandate of an entity, such organization continues to be the PIC.[6]

Considering the above discussion, it then follows that the scope and limitation of the processing activities to be performed by AFPI should be clearly defined in the Outsourcing Agreement. It is the duty of the PIC to ensure that the contract contains all the provisions discussed in Rule 10 of the Implementing Rules and Regulations (IRR) of the DPA and issuances of the NPC, particularly on the required security measures and personal data breach management.

---

[3] Republic Act No. 10173, §3(i).
[4] Amending Executive Order No. 125, Entitled "Reorganizing the Ministry of Transportation and Communications, Defining its Powers and Functions, and For Other Purposes", [REORGANIZATION ACT OF THE MINISTRY OF TRANSPORTATION AND COMMUNICATIONS], Executive Order No. 125-A, (1987), §5.
[5] Data Controllers and Data Processors: What the difference is and what the governance implications are, pages 4 and 7, available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, (last accessed on 07 June 2018).
[6] Id, page 5.

As to the role of the PTOs in the AFCS, there is a need to clarify and define their obligations with respect to its contract with AFPI vis-à-vis the AFCS Concession Agreement between DOTr and AFPI.

Finally, we wish to emphasize that should AFPI and/or the PTOs use the personal data collected for purposes other than the processing for the issuance of the Concessionary beep™ Cards or as instructed by the DOTr pursuant to the AFCS Concession Agreement, they risk violating the law. In these cases, they are to be considered as PICs with respect to the personal data being processed outside the agreement with DOTr. To do this lawfully, the processing must be based on consent or some authority provided by law and regulation. The criteria for lawful processing is provided in Section 12 and 13 of the DPA.

This opinion is being rendered based on the limited information you have provided. The NPC is not cognizant of the contents of the AFCS Concession Agreement, the full scope of work of AFPI as well as the extent of the responsibilities of PTOs in this endeavor. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-039

27 July 2018

[redacted]

RE: RIGHT TO ERASURE IN RELATION TO RETENTION OF PERSONAL INFORMATION

Dear [redacted],

We write in response to your inquiry requesting for a clarification with regard to NPC Advisory Opinion No. 2017-024 on retention of personal data under Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA). Specifically, you seek to clarify the following:

a. Whether a resigned employee may request that all his personal data kept by the former employer be deleted;
b. Whether a resigned employee may demand the turnover of the compilation of his personal data under the employer's custody; and
c. Possible valid reasons for an employer to deny the above requests.

Rights of the data subject

Section 16 of the DPA clearly sets forth the right of every data subject to suspend, withdraw or order the removal or destruction of personal information from the filing system of a personal information controller (PIC) upon discovery and substantial proof that the personal information is outdated or is no longer necessary for the purposes for which they were collected, among other conditions.

Thus, it is possible for employees as data subjects to request for deletion of their personal data held by former employers. Note however that this right is not absolute and is subject to existing laws and regulations governing the retention period of employment documents or records.

[1] 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).

Section 34(e) of the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that this right may be exercised upon discovery and substantial proof of any of the following:

1. The personal data is incomplete, outdated, false, or unlawfully obtained;
2. The personal data is being used for purpose not authorized by the data subject;
3. The personal data is no longer necessary for the purposes for which they were collected;
4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
5. 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;
6. The processing is unlawful; and
7. The personal information controller or personal information processor violated the rights of the data subject.

Likewise, employees as data subjects have the right to reasonable access to personal data subject to processing by the PIC. This includes reasonable access to the following:

1. Contents of his or her personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
7. Date when his or her personal information concerning the data subject were last accessed and modified; and
8. The designation, or name or identity and address of the personal information controller.[2]

The employee may exercise his or her right to reasonable access by requesting for copies of the information comprising his or her personal data from the employer.

[2] Id., § 16(c).

As to turnover of employees' personal data, the question contemplates two situations where different rights may apply. On one hand, if the employer merely provides copies of the records to the employees, he complies with the right to access by acceding to the data subjects' requests for their respective personal data. On the other hand, if the employer transfers the records in their custody to the former employee, this fulfills the employee's right to erasure because the records are effectively deleted or removed from the database of the employer.

Nonetheless, turning over of the employee's compiled personal data upon cessation of employment may not be possible in instances where the PIC has a legitimate purpose to retain the same.

Retention period of records

The DPA allows the employer to retain personal data of employees for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law.[3]

As stated in NPC Advisory Opinion No. 2017-24, factors that may be considered by a company in determining retention periods of employment records would include, but are not limited to the following:

1. Legal requirements to which the company may be subject;
2. Applicable prescription periods in existing law (i.e., money claims);
3. Department of Labor and Employment rules;
4. Bureau of Internal Revenue regulations; and
5. Industry standards and other laws and regulations that apply to the sector.

Thus, the above-mentioned may be used by the employers as ground for denial of requests for deletion of employee records and requests for turnover of the same. Notwithstanding the circumstances, the employees shall not be hindered from exercising their right to access and obtain copies of their personal data.

Lastly, the company should be mindful of the data privacy principles of transparency, legitimate purpose and proportionality. This means that employees must be informed of the basis and purpose for the retention of his or her employment records. Further, the company must ensure

[3] Id., §11(e).

that only those personal data which is adequate, relevant, suitable and necessary for the purpose will be retained.[4]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[4] Id., §11.

ADVISORY OPINION
NO. 2018-040

11 October 2018

[redacted]

RE: PUBLICATION OF NAMES OF SANCTIONED DIRECTORS AND OFFICERS OF BSP-SUPERVISED FINANCIAL INSTITUTIONS

Dear [redacted],

We write in response to your request for an advisory opinion on your practice of publishing the names of sanctioned directors and officers of Bangko Sentral ng Pilipinas (BSP)-supervised financial institutions (BSFIs) for their failure to address BSP requirements and supervisory expectations.

Section 4 of Data Privacy Act of 2012[1] (DPA) states that the law is applicable to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. However, it provides for certain exemptions – one of which is personal data necessary in order to carry out the functions of public authority, including the processing of personal data for the performance by the independent, central monetary authority of its constitutionally and statutorily mandated functions.[2]

As Section 3 of Republic Act No. 7653, or the New Central Bank Act, charged the BSP with supervising operations of banks and exercise such regulatory powers as provided for by the New Central Bank Act and other pertinent laws over the operations of finance companies and non-bank financial institutions performing quasi-banking functions, and institutions

[1] 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).
[2] Id. § 4 (e).

performing similar functions, which necessarily includes the issuances of directives and enforcement actions, it satisfies this provision in the DPA.[3]

The DPA has the twin task of protecting the fundamental human right of privacy and ensuring the free flow of information to promote innovation and growth.[4] For this reason, the DPA will not operate to hinder the BSP to disclose certain information it deems crucial that the public be informed of, anchored on its mandate to maintain financial stability, as enforced by Circular No. 875, dated 15 April 2015.[5]

Likewise, the following quasi-judicial administrative bodies also publish its decisions, including the names of individuals that are the subject of or involved in the cases:

- Civil Service Commission on cases involving public officials and employees;[6]
- Commission of Audit;[7]
- Bureau of Internal Revenue on tax evasion cases;[8] and
- Securities and Exchange Commission.[9]

Similar lists are also published by the Asian Development Bank (ADB) and the World Bank. The ADB publishes on its website a sanctions list of individuals and entities who violated its anticorruption policies.[10] Also, the World Bank publishes a list of ineligible firms and individuals who have been sanctioned under the Bank's fraud and corruption policy.[11]

The business of banking is imbued with public interest. The stability of the banking industry largely depends on the confidence of the people in the honesty and efficiency of banks and the people managing the banks. Thus, BSP has a legitimate purpose in making the public aware of sanctions imposed by BSP through its publication.

---

[3] Bangko Sentral ng Pilipinas, Overview of Functions and Operations, available at http://www.bsp.gov.ph/about/functions.asp, (last accessed on 24 May 2018).

[4] Supra note 1., § 2.

[5] Bangko Sentral ng Pilipinas (BSP) Supervisory Enforcement Policy

[6] See: Civil Service Commission Must-read Resolutions available at http://www.csc.gov.ph/2014-02-21-08-28-23/pdf-files/category/38-must-read-resolutions (last accessed 19 July 2018).

[7] See: Commission on Audit Legal Information Archive available at https://lia.coa.gov.ph/browse/5 (last accessed 19 July 2018).

[8] See: Bureau of Internal Revenue RATE Cases available at https://www.bir.gov.ph/images/bir_files/old_files/pdf/ratex.pdf (last accessed 19 July 2018).

[9] Securities and Exchange Commission Decisions available at http://www.sec.gov.ph/public-information-2/sec-issuances/securities-and-exchange-commission-decisions/ (last accessed 19 July 2018).

[10] Asian Development Bank Anticorruption and Integrity Published List available at https://lnadbg4.adb.org/oga0009p.nsf/sancALL1P?OpenView&count=999 (last accessed 29 July 2018)..

[11] http://web.worldbank.org/external/default/main?contentMDK=64069844&menuPK=116730&pagePK=64148989&piPK=64148984&querycontentMDK=64069700&theSitePK=84266 (last accessed 29 July 2018).

Extent of exemption

However, it should be noted that the exemptions set forth in the DPA are limited to the minimum extent necessary to achieve the specific purpose, function or activity. The BSP, in processing personal data, assumes the role of a personal information controller (PIC),[12] which is required by the DPA to take all measures necessary to protect personal data.

Furthermore, said publication should also adhere to the principle of proportionality especially since it would involve public disclosure of personal information. The principle requires that "the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if purpose of the processing could not reasonably be fulfilled by other means.[13]

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[12] Data Privacy Act of 2012, § 3 (h).
[13] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

ADVISORY OPINION
NO. 2018-41

9 August 2018

[redacted]

RE: PASIG CITY ORDINANCE NO. 51

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission for clarification on Pasig City Ordinance No. 51, series of 2017 (Ordinance).

Section 77 of said Ordinance requires human resource officers/heads or owners of business establishments as well as administrative officers of national government units including government-owned and controlled corporations in Pasig City to submit not later than the 15th of May of each year a list of persons under their employ stating therein the following:

1. Name and address;
2. Total salaries, wages and allowances of preceding year;
3. Community Tax Certificate number, date, place of issue and amount paid; and
4. Tax Identification Number.

In view of the foregoing requirement, you asked the following:

- Is there a need to secure the consent of each of the employees who will be included in the list prior to submission to the City Government?
- Do we need to execute a Data Sharing Agreement with the City Government in relation to the information being requested?

Lawful processing of personal data

Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR) applies to the processing of all types of personal information and to any natural and juridical person in the government or private sector.

Personal information is defined by the law as "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." [2]

The law then further categorizes certain personal information as sensitive personal information, which includes personal information issued by government agencies peculiar to an individual such as the Community Tax Certificate (CTC) number and Tax Identification Number (TIN). [3]

The Ordinance requires the CTC number and TIN of the employee to be included in the list. These are sensitive personal information the processing of which is prohibited except for certain cases stated under Section 13 of the DPA, to wit:

> "SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx xxx xxx
>
> b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;"

Hence, the consent of the employees may no longer be required when your company submits the list pursuant to the Ordinance as consent is not the basis for processing.

[1] 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).
[2] Data Privacy Act of 2012, §3(i).
[3] Id., §3(l)(3).

Nonetheless, we wish to remind you of the data privacy principle of transparency which dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, his or her rights as a data subject, and how these can be exercised.[4] The data subject is entitled to be informed whether personal information pertaining to him or her shall be, are being or have been processed.[5]

The above may be may be operationalized through a privacy notice. A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[6] It is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.[7]

Data sharing agreement

Considering that an existing law, not consent, is the basis for the processing of personal data, the execution of a data sharing agreement with the City Government is not a condition precedent for the submission of the personal data required by the Ordinance. This is pursuant to Section 1 of NPC Circular 16-02 relating to Data Sharing Agreements involving Government Agencies, which states that "nothing in this Circular shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law." Nonetheless, to ensure that there are adequate safeguards for data privacy and protection, the City Government should issue the necessary guidelines to operationalize the transfer of personal data from the covered entities, following the principles, provisions and security measures required under NPC Circular 16-02.

We trust also that the City Government, as a personal information controller, is well aware of its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, which requires all government agencies engaged in the processing of personal data to observe the following duties and responsibilities:

A. through its head of agency, designate a Data Protection Officer;
B. conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data, Provided, that such assessment shall be updated as necessary;
C. create privacy and data protection policies, taking into account

[4] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18(a).
[5] Data Privacy Act of 2012, §16(a).
[6] IAPP, Glossary of Privacy Terms, available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2
[7] Id.

the privacy impact assessments, as well as Sections 25 to 29 of the IRR;

D. conduct a mandatory, agency-wide training on privacy and data protection policies once a year: Provided, that a similar training shall be provided during all agency personnel orientations.
E. register its data processing systems with the Commission in cases where processing involves personal data of at least one thousand (1,000) individuals, taking into account Sections 46 to 49 of the IRR;
F. cooperate with the Commission when the agency's privacy and data protection policies are subjected to review and assessment, in terms of their compliance with the requirements of the Act, its IRR, and all issuances by the Commission.[8]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[8] NPC Circular No. 16-01 dated 10 October 2016, §4.

ADVISORY OPINION
NO. 2018-42

7 August 2018

[redacted]

RE: EMPLOYEE'S RIGHT TO ACCESS EMPLOYMENT RECORDS

Dear [redacted],

This is in response to your inquiry received by the National Privacy Commission (NPC) regarding the employee's right to access his employment records, pursuant to Section 16 of Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA). Specifically, you are seeking clarification on the following:

1. Whether an employee can request for a copy of the results (laboratory exam results, ECG paper or x-ray film) of his annual physical exam conducted by the company for personal use;
2. Whether an employee may request for a copy of his 201 file, including the trainings attended or results of performance evaluation; and
3. Whether the resigned employee may request for a copy his personal data and other records retained by the company.

Processing of personal data of employees

It is a fact that processing of personal data at work is inevitable and indispensable. The collection, use and retention of personal data of employees is necessary for the performance of a contract, compliance with a legal obligation, in furtherance of the employer's legitimate interests or when the employee expressly gives his or her consent to the personal information controller for processing.[2]

[1] 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).
[2] Id, §12 and 13.

Nevertheless, the employers, as personal information controllers (PICs), are directed to adhere to the principles of transparency, legitimate purpose and proportionality in the collection, processing, retention, storage and disclosure of personal information in their custody.[3]

Right to reasonable access of personal information

The employee as a data subject may exercise his or her right to reasonable access to the following:

1. Contents of his or her personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis of any decision significantly affecting or will affect the data subject;
7. Date when his or her personal information concerning the data subject were last accessed and modified; and
8. The designation or name or identity and address of the personal information controller.

In some instances, copies of personal data retained by the employer may be requested by the employee, particularly those records that are provided by the employee upon application and those related to his or her official duties and responsibilities.[4] However, some personnel files that are obtained in confidence shall be kept confidential and the employer may withhold disclosure, reproduction or viewing of the particular file.[5]

As an alternative, perhaps it is possible for the employer to provide a summary of the confidential information without causing prejudice to its interests or other parties involved.[6]

---

[3] Id, §11.

[4] Repa, Barbara Kate. State Laws on Access to Your Personnel File, available at https://www.nolo.com/legal-encyclopedia/free-books/employee-rights-book/chapter5-2.html, last accessed on 26 July 2018.

[5] Privacy at Work: A Guide to the Privacy Act for employers and employees, Office of the Privacy Commissioner of New Zealand, available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf, last accessed on 26 July 2018.

[6] Id.

Access to results of the annual physical exam

Medical records are classified as sensitive personal information and are then treated with utmost care and strict confidentiality.

In the given scenario, we assume that the company sponsored and shouldered the cost for the annual physical exam and the attendant laboratory procedures. Nonetheless, the employee has the right to access and ask for a copy of the results and related documentation, subject to existing company protocol on accessing employee files.

Access to personnel file

Employees are generally allowed reasonable access to their files, specially those they have personally provided the employer during the recruitment and application process.

The trainings attended by the employee may be disclosed since they are part of the duties, responsibilities and privileges attached to the position and function and part of the professional development and capacity building program of the employer.

As to access to employee performance evaluation, it may be viewed in two perspectives. If the evaluative material is solely complied to determine the qualification of the employee for employment, appointment, promotion, recognition or termination, and such is given by the immediate supervisor due to the normal course of personnel evaluation, the employee is entitled to know the rating.[7]

On the other hand, if the evaluative material is given in confidence, in such a way that the rating and observation will not be given except for an understanding of confidentiality and anonymity, the employee shall not be permitted to access the file.[8]

Nonetheless, the employer may likewise provide a summary of all the ratings given to the employee without identifying the source in order to uphold the duty of confidentiality.

Access to personal data after resignation

Upon cessation of employment, the employer may retain the records and files of the employee in accordance with the retention period as

[7] Supra note 5.
[8] Id.

may be provided for by existing laws on the matter and/or as stated in its policies.

If the request falls within the retention period of employment records, the employer shall provide reasonable access to the requested information, subject to the same limitations discussed above and its own company policies.

Please note that as part of the organizational security measures, PICs are required to develop, implement and review policies and procedures for data subjects to exercise their rights under the DPA.[9]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[9] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016), §26(e)(4)

ADVISORY OPINION
NO. 2018-43

7 August 2018

[redacted]

RE: REGISTRATION OF DATA PROCESSING SYSTEMS

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought to clarify matters regarding Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR)[2] and relevant issuances, particularly NPC Circular No. 17-01.

You requested for clarification on whether the processing of personal information in Microsoft Office 365 (Office 365) is considered as a data processing system. If in the affirmative, whether the following entities are required to register with the NPC:

1. A corporation (Foreign Parent) registered outside of the Philippines, engaged in manufacturing and distribution of control equipment, factory automation systems and electronic components, having no employees in the Philippines and not processing sensitive personal information of at least one thousand (1,000) individuals who are located in the Philippines or are Philippine citizens; and

2. A subsidiary of the Foreign Parent (Asia Affiliate), also engaged in the same business of the Foreign Parent, and its representative office registered in the Philippines (Rep Office), where the latter has twenty (20) employees.

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173.

Data processing system

We understand that the Foreign Parent plans to introduce Office 365 globally to its branches and affiliates (Group). The same will be used to achieve operational efficiency within the Group. Personal information of the employees such as names, email addresses, and other information voluntarily provided by said employees may be processed and shared with the Group.

We confirm that Office 365 and its allied applications may be considered as a data processing system, defined as 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.[3]

Registration

For the registration requirement, NPC Circular No. 17-01 and its Appendix 1 must be read together with the law and its IRR. Section 3 of the DPA provides for the definition of processing of personal data which refers to any operation or any set of operations performed upon personal information, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

In connection with this, the natural or juridical person who may be required to register are those operating and doing business in the Philippines. Doing business is understood as it is defined under Executive Order No. 226, as amended, or the Omnibus Investment Code of 1987, the Foreign Investments Act of 1991, as amended, the respective IRRs, as amended, and other applicable laws, rules, regulations and jurisprudence on the matter.

This is read in conjunction with Section 46 (a) of the IRR, which provides as follows:

> "Section 46. Enforcement of the Data Privacy Act. Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the following:

[3] NPC Circular No. 17-01 - Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making, 31 July 2017, §3(F).

a. Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;"

From the foregoing, the registration requirement is interpreted to apply to those natural or juridical persons operating and doing business in the Philippines and where such business activity involves the processing of personal data through data processing systems operating in the Philippines.

A foreign corporation that does not operate or do business in the Philippines and does not process personal data through data processing systems operating in the Philippines are not covered by the mandatory registration requirement.

Nevertheless, the Foreign Parent and Asia Affiliate, through its Rep Office may always opt to avail of the voluntary registration provided under Section 6 of NPC Circular No. 17-01.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-044

7 August 2018

[redacted]

RE: REQUEST FOR INFORMATION FROM RIZAL MEDICAL CENTER

Dear [redacted],

We write in response to your email dated 3 August 2018 received by the National Privacy Commission (NPC), attaching a handwritten request for advisory opinion on the above captioned matter, specifically, on the request addressed to Rizal Medical Center (RMC) to release the following information:

1. Actual date/time of alcohol test conducted;
2. Actual date/time of drug test conducted; and
3. Names of doctors/lab personnel for tests.

This is also with reference to the previous report dated 17 July 2018 sent by the Contact Center ng Bayan of the Civil Service Commission (CSC) through email. Said report (Request for Assistance – For Immediate Action) provided details on your letter request dated 20 June 2018 addressed to the RMC for "an Official Copy of the Alcohol and Drug Test Results" of a certain Luis O. Asistio III, and the RMC's letter reply dated 6 July 2018.

We understand that the RMC denied the request on the basis of patient confidentiality and the provisions of the Data Privacy Act of 2012 (DPA).[1]

Legitimate purpose; Lawful processing; Disclosure to a third party of personal data held by a hospital should have patient's consent or should be authorized under existing laws and regulations.

[1] 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).

The NPC has been requested to issue an advisory opinion on whether a hospital can disclose the fact that diagnostic exams or chemical tests have been performed on an individual in the health facility. In this particular case, a third party asks a public hospital to disclose whether an alleged suspect in a vehicular accident, reported to have resulted in the loss of human life, had an alcohol test or drug test performed in the health facility. It is not clear whether the alleged suspect is a patient of the facility, and whether cases have been brought against him.

For purposes of this advisory opinion, we took note of the letter of the RMC addressed to the requesting party. This letter was received by NPC from the CSC on July 17, 2018. The said letter informed the requesting party that the hospital "cannot release or share medical records because we are bound by patient confidentiality and provisions of RA No. 10173 or the Data Privacy Act." This letter is considered in addition to the information provided by requesting party through telephone conversations.

Based on the present inquiry, the information on the alcohol test or drug test is being requested for the purpose of finding out if the provisions of R.A. No. 10586[2] have been complied with. The relevant provisions in the said law are:

> Section 7. Mandatory Alcohol and Chemical Testing of Drivers Involved in Motor Vehicular Accidents. – A driver of a motor vehicle involved in a vehicular accident resulting in the loss of human life or physical injuries shall be subjected to chemical tests, including a drug screening test and, if necessary, a drug confirmatory test as mandated under Republic Act No. 9165, to determine the presence and/or concentration of alcohol, dangerous drugs and/or similar substances in the bloodstream or body.
>
> Section 8. Refusal to Subject Oneself to Mandatory Tests. – A driver of a motor vehicle who refuses to undergo the mandatory field sobriety and drug tests under Sections 6, 7 and 15 of this Act shall be penalized by the confiscation and automatic revocation of his or her driver's license, in addition to other penalties provided herein and/or other pertinent laws.[3]

As a general rule, the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in

[2] An Act Penalizing Persons Driving Under the Influence of Alcohol, Dangerous Drugs, and Similar Substances, and for Other Purposes [Anti-Drunk and Drugged Driving Act of 2013] Republic Act No. 10586, (2013).
[3] Anti-Drunk and Drugged Driving Act of 2013, §§ 7-8.

personal information processing.[4] It allows the processing of personal information, subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.[5]

These provisions mean that a hospital, whether private or public, is covered by the DPA, and the provisions of the law apply to the processing of personal information, sensitive personal information and privileged information in the health care facility.

In this inquiry, a third party is asking the hospital to disclose personal information, which is any information which relates to an identified or identifiable person. The identity of the patient and the fact that a particular diagnostic test has been performed, are personal information.

Information about whether a diagnostic test has been performed is already information with clinical value because it is no longer limited to just the general information like name of patient, address, attending physician and admission and discharge dates.[6]

The fact of ordering a diagnostic test or chemical test may already disclose information about a patient's medical condition. This already goes into the differential diagnosis of a physician, which is based on a patient's history, presenting symptoms, physical examination, and the professional judgment of the physician. This information is already part of the physician-patient relationship, the medical management, and involves advice, treatment and information acquired in the course of attending to a patient. There is no information available to evaluate whether the requested information falls under any category of information other than that which may have been acquired by the hospital in the context of provision of healthcare.[7]

The processing of all types of personal information will be allowed if the processing, such as disclosures to third party, complies with the requirements of the DPA, including the mandatory requirement of meeting at least one of the criteria for lawful processing.

---

[4] Data Privacy Act of 2012, § 4.
[5] Id., § 11
[6] DOH Health Information Manual (2013), p. 37.
[7] It should be noted that even under the Dangerous Drugs Board Regulation No. 2 Series of 2003, Subject: Implementing Rules and Regulations Governing Accreditation of Drug Testing Laboratories in the Philippines:
15.4. Access to laboratory test results – the drug test result and the records shall be confidential subject to the usual accepted practices to protect the confidentiality of the test results.

Under Sections 12 and 13 of the DPA:

Section 12. **Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists**:

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Section 13. **Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:**

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: **Provided,** That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: **Provided, further,** That the

consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: **Provided,** That such processing is only confined and related to the **bona fide** members of these organizations or their associations: **Provided, further,** That the sensitive personal information are not transferred to third parties: **Provided, finally,** That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[8]

Based on the information provided in this particular inquiry, the requested disclosure of personal information to a third party does not meet any of the criteria provided by the DPA in Sections 12 and 13. It should be emphasized that the request for disclosure in this instance is from a third party, an individual other than a patient or a patient's authorized representative. The request is also not being made by a public authority for the fulfillment of their functions, nor does it proceed from a duly issued subpoena or court order. The information requested also pertains to a patient's health, with clinical value, and is considered sensitive and privileged in nature, the processing of which is prohibited except under specific circumstances.

The purpose for requesting the information should be examined. Hospitals are bound by reporting requirements in many instances, where disclosures are provided by law and regulation.

[8] Data Privacy Act of 2012, §§ 12-13 (emphasis supplied).

At the onset, it should be clear that nothing in the Anti-Drunk and Drugged Driving Act of 2013 or its Implementing Rules and Regulations (IRR) provide for the reporting requirement on the part of hospitals to disclose information relevant to diagnostic tests it performs in its facilities.

Likewise, Section 7 of the Anti-Drunk and Drugged Driving Act of 2013 does not impose the obligation to conduct mandatory alcohol and chemical testing of drivers on the hospital.

On the other hand, Section 6 of the same law provides, "If the law enforcement officer has probable cause to believe that a person is driving under the influence of dangerous drugs and/or other similar substances, **it shall be the duty of the law enforcement officer** to bring the driver to the nearest police station to be subjected to a drug screening test and, if necessary, a drug confirmatory test as mandated under Republic Act No. 9165."[9]

Furthermore, Rule IV of the IRR of R.A. No. 10586 provides:

> RULE IV – MANDATORY ALCOHOL AND DRUG TESTING
>
> Section 1. Mandatory Alcohol and Chemical Testing of Drivers Involved in Motor Vehicular Accidents
>
> a. A driver of a motor vehicle involved in a vehicular accident resulting in the loss of human life or physical injuries shall be subjected to on site field sobriety test and ABA testing, whenever practicable, and, thereafter chemical tests, including a drug screening test and, if necessary, a drug confirmatory test as mandated under Republic Act No. 9165, to determine the presence and/or concentration of alcohol, dangerous drugs and/or similar substances in the bloodstream or body. A LEO may use other alcohol testing equipment, such as Gas Chromatography-Mass Spectroscopy (GCMS), whenever the use of an ABA is not practicable under prevailing circumstances.
>
> b. A driver of a motor vehicle who refuses to undergo the mandatory testing as required shall be penalized by the confiscation and automatic revocation of his or her driver's license, in addition to other penalties provided herein and/or other pertinent laws.[10]

The term LEO "refers to law enforcement officers of the LTO or authorized

[9] RA No. 10586, §6.
[10] Rules and Regulations Implementing the Anti-Drunk and Drugged Driving Act of 2013, Republic Act No.10586, Rule IV, § 1.

officer trained and deputized by the Land Transportation Office to **enforce the provisions of this Act."**[11] Under said law, the duty to ensure that the provision is complied with attaches to the law enforcement officers, depending on the circumstances of the case.

No similar duty has been imposed on the hospital under the Anti-Drunk and Drugged Driving Act of 2013 or its IRR. More so, the disclosure by the hospital to a third party of such personal data is not provided for by existing laws and regulations. In fact, if abovementioned Section 7 is read together with Section 8 of R.A. No. 10856, it will likewise be clear that an individual may refuse to undergo the mandatory field sobriety and drug tests, but he or she will be subjected to penalties. This means that should the individual refuse to comply with the mandatory requirement, corresponding penalties are imposed by the law on the individual refusing the tests. The penalty is not imposed on hospitals.

The purpose of the request is to determine whether the provisions of R.A. No. 10586 have been complied with. This may be accomplished by other means, without unnecessarily overturning the duty of confidentiality of healthcare providers, and the rule on privileged communications.

The information requested by the third party may be obtained from the hospital, either with consent of the patient, or when authorized by law or regulation. The duty of confidentiality on the part of healthcare providers is more than a legal obligation but also an ethical one. This is fundamental to a physician-patient relationship, which is fiduciary in nature and dependent on trust.

Disclosures of health information are allowed but only under specific circumstances, considering the identity of the requesting party, the purpose of the request, and any applicable legal obligations. Disclosures must be based on law and regulation and cannot be arbitrarily made.

In the absence of clear legal requirements authorizing the disclosure of the requested information under the circumstances of this inquiry, the hospital is not obligated to release any health information to the requesting party, including the fact of whether any diagnostic or chemical tests have been done.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

[11] Id., Rule I, § 3 (n).

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-045

13 August 2018

[redacted]

Re: RIGHT TO ACCESS CLINICAL INFORMATION OF PATIENTS

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) which sought to clarify whether the approval of the attending physician is required before a patient can be given access to their clinical information. Specifically, you are asking for clarification whether the following provisions in Department of Health (DOH) Hospital Health Information Management Manual 3rd Edition[1] is consistent with the provisions of the Data Privacy Act of 2012 (DPA):[2]

"From a Patient

- Ask the patient for identifying information and find out what he wishes to know.
- Only the following data can be given directly to the patient without the approval of the attending physician: admission and discharge dates, name of the attending physician, and other demographic data except any clinical information.
- If an approval has been obtained from the attending physician, the patient may have the right to access all the clinical information needed."

We understand that the above provisions refer to the procedures for the release of information over the phone.

[1] Hospital Health Information Management Manual-Third Edition (formerly Hospital Medical Records Management Manual), National Center for Health Facility Development (NCHFD), (2010).
[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).

Data subject's right to access

Under Section 16(c) of the DPA, the data subject is entitled to reasonable access to, upon demand, the following:

1. Contents of his or her personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
7. Date when his or her personal information concerning the data subject were last accessed and modified; and
8. The designation, or name or identity and address of the personal information controller.

The healthcare provider/institution may prescribe the procedure and form to facilitate the efficient handling of such access requests, taking into consideration other existing laws, policies, and guidelines. We note also that as part of the organizational security measures, personal information controllers (PICs) are required to develop, implement and review policies and procedures for data subjects to exercise their rights under the DPA.[3]

The personal data relevant to the request must be provided by the PIC to the data subject or his authorized representative through a written document, or by any other format practicable to the PIC, including, where appropriate, by electronic means.[4]

To reiterate the provision that you referred to from the DOH Manual, it is important to note that the said provision pertains specifically to the handling of telephone inquiries. Hence, the condition should not be inferred to as a general statement or standard procedure in handling all types of access requests. Thus, there is no incompatibility between the DOH's rule in handling telephone inquiries and the DPA.

Healthcare facilities may prescribe the manner through which access requests may be made. In implementing reasonable and appropriate organizational, technical, and physical security measures to ensure the

[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016), §26(e)(4)

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [EU GENERAL DATA PROTECTION REGULATION], Article 12 (2016).

confidentiality, integrity and availability of personal data, PICs should consider measures which uphold the data subject's right to access.

The provisions you have cited serves as a security measure to protect the sensitive personal information of the patient, such as health/clinical information, from unauthorized access, especially when the information is being requested over the phone where the identity of the caller is not apparent.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-46

13 August 2018

[redacted]

Re: CONSENT FOR BUSINESS CORRESPONDENCE

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) regarding consent for business correspondence. Specifically, you asked if business contact information on business cards is within the scope of Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA), and if written consent is needed when a person offers their contact information.

Scope of the DPA; criteria for lawful processing of personal information

The DPA applies to the processing of all types of personal information and to any natural and juridical persons involved in personal information processing.[2] Business contact information on business cards is personal information which is not of a sensitive nature, and the collection thereof is considered as a processing activity.[3]

Processing of personal information shall be permitted when the data subject has given his or her consent, or when processing is necessary and related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract, or when it is necessary for the legitimate interest of the personal information controller (PIC), among others.[4]

[1] 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).
[2] Id., §4.
[3] Id. §3(j).
[4] Id. §12.

Organizations or individuals can use and store personal information as reflected on the business cards even without consent of the data subject as long as the processing activity is part of the normal business correspondence. In this instance, processing may be considered as being pursuant to the legitimate interest of the entity or the recipient of the personal information.

Legitimate interests of the personal information controller

Section 12(f) of the DPA provides that the processing of personal information shall be permitted when the processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Recital 47 of the EU General Data Protection Regulation (GDPR) states that legitimate interests of a controller may provide a legal basis for processing taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.[5]

Further, the Recital stated that such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.[6]

From the foregoing, the processing of business contact information on business cards may be based on the legitimate interest of the PIC to whom such contact information was provided.

However, if the personal information will be further processed in a way not compatible with the original business purpose or beyond the data subject's reasonable expectations on the processing of their personal data, consent may be required.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [EU GENERAL DATA PROTECTION REGULATION], Recital 47 (2016).
[6] Id.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-047

15 August 2018

[redacted]

Re: DISCLOSURE OF CERTIFICATE OF LIVE BIRTH

Dear [redacted],

We write in response to your inquiry received by the National Privacy Commission (NPC) via email.

We understand that you received a subpoena requiring you to appear in relation to an investigation regarding the alleged falsification and perjury in connection with the Certificate of Live Birth (Certificate) of your daughter. During the hearing, you were presented with a copy of the said Certificate which was requested from the Civil Registrar in your municipality.

In addition, you likewise mentioned that a portion of the said Certificate was posted on social media (Facebook) which showed the name of the child and the father, among others.

You now inquire whether a violation of the Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA), has been committed in the given scenario.

Acquisition of the Certificate of Live Birth for a Court Proceeding

The DPA and its Implementing Rules and Regulations (IRR) applies to the processing[2] of all types of personal information and to any natural and juridical person in the government or private sector.[3] Personal information

[1] 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).
[2] Id. § 4 - Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 4 (2016).

is defined by the law as "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."[4] The law then further categorizes certain personal information as sensitive personal information, which among others, includes an individual's race, ethnic origin, age, color and religion.[5]

The Certificate contains the following information of an individual: name, sex, date of birth, place of birth, citizenship, and religion, among others. By its very nature, the certificate issued by the Civil Registrar contains sensitive personal information.

As decreed by the DPA and its IRR, the processing of sensitive personal information is prohibited except for certain cases stated under the law.[6] One exception is when sensitive personal information is processed because it is provided to government or public authority pursuant to a constitutional or statutory mandate.

In the case of certificates of live birth, Presidential Decree No. 603, otherwise known as The Child and Youth Welfare Code, applies. Thus:

> Article 7. Non-disclosure of Birth Records. - The records of a person's birth shall be kept strictly confidential and no information relating thereto shall be issued except on the request of any of the following:
>
> (1) The person himself, or any person authorized by him;
> (2) His spouse, his parent or parents, his direct descendants, or the guardian or institution legally in-charge of him if he is a minor;
> (3) The court or proper public official whenever absolutely necessary in administrative, judicial or other official proceedings to determine the identity of the child's parents or other circumstances surrounding his birth; and
> (4) In case of the person's death, the nearest of kin.[7]

In the given situation, the subject of the court proceeding was the alleged falsification and perjury in connection with the Certificate of Live Birth of your daughter. The crimes of falsification and perjury necessarily pertain

[4] Id. § 3 (l).
[5] Id. § 3 (t) (1).
[6] Id. § 22.
[7] Emphasis supplied.

to alleged falsified information stated in the certificate. Such information may relate to the parents' identity or other circumstances surrounding the birth of your daughter. Hence, the acquisition of the Certificate of Live Birth and its successive disclosure made to the court is specifically allowed under prevailing law.

Unlawful Disclosure of Sensitive Personal Information

With respect to the posting without consent of the contents of the Certificate of Live Birth on Facebook, the following are the possible violations penalized by imprisonment and fine under the DPA:

> Section 58. Malicious Disclosure. Any personal information controller or personal information processor, or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).
>
> Section 59. Unauthorized Disclosure. xxx xxx xxx
>
> b. Any personal information controller or personal information processor, or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

This opinion is being rendered based solely on the limited information you have disclosed. Additional information may change the context of the inquiry and the appreciation of the facts. It shall be understood that this opinion shall not be binding upon the Commission or the courts in other cases. Should the matter be raised as a complaint, the Commission shall render its decision upon further inquiry and investigation, and due appreciation of established facts and circumstances in accordance with the Rules of Procedure under NPC Circular 16-04.

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-049

26 November 2018

[redacted]

Re: DISCLOSURE OF PERSONAL INFORMATION TO THE POLICE AND THE MEDIA

Dear [redacted],

We write in response to your queries received by the National Privacy Commission (NPC) concerning the disclosure of personal information of patients to police officers and the media and how one would balance crime prevention, detection, and investigation vis-à-vis patient's right to data privacy.

In your email, you stated that the police interview or obtain information about patients who are either alleged perpetrators of a crime or victims thereof. Also, you asked the following questions regarding disclosure to the media:

1. When dealing with media people, how do we balance patient privacy and public's right to know?
2. Do we have a legal obligation to disclose information to the media?
3. Do the media have the legal mandate to compel institutions like hospitals to disclose information?

Disclosure to the police in relation to a criminal investigation

The Data Privacy Act of 2012 (DPA)1 is a law that involves primarily one aspect of privacy, that of information privacy. Strictly, the DPA does not include in its coverage hospital policies that pertain to hospital operations

[1] 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).

including procedures in dealing with law enforcement, except to the extent that they relate to the protection of personal data.

The DPA states that the processing of personal information shall be allowed, subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.[2]

In general, a hospital should not release health information about patients unless with their consent or with authority of law. For personal information, which may include the name of patient, address, date and time of admission, this may be disclosed subject to Section 12 (d)(e)(f), to wit:

> "(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."

For sensitive health information, release is generally prohibited unless it is permitted by specific provision of law. The following provisions in Section 13 of the DPA may be applicable:

> "(b) The processing of the same is provided for by existing laws and regulations: ***Provided,*** That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: ***Provided, further,*** That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of

[2] Data Privacy Act of 2012, § 11.

the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority."

Relative to the abovementioned provisions, the Philippine National Police (PNP) has the following powers and functions, as enumerated in Section 24 of Republic Act No. 6975:[3]

a. Enforce all laws and ordinances relative to the protection of lives and properties;
b. Maintain peace and order and take all necessary steps to ensure public safety;
c. Investigate and prevent crimes, effect the arrest of criminal offenders, bring offenders to justice and assist in their prosecution. (underscoring supplied)

Thus, the disclosure of personal information of patients to law enforcement officers may be allowed under the DPA when it is pursuant to its mandate to investigate and prevent crimes, and strictly following the existing standard operating procedures in the conduct of an investigation and law enforcement operation as stated in the Revised PNP Operational Procedures, and other pertinent laws, rules, and regulations governing the same (i.e. criminal procedures on search and seizure, etc.) Only these contexts do the exercise of a mandate becomes a lawful basis for processing.

Investigation refers to the collection of facts to accomplish a three-fold aim: (a) to identify the suspect, (b) to locate the suspect, and (c) to provide evidence of his guilt. In the performance of his duties, the investigator must seek to establish the six (6) cardinal points of investigation, namely: what specific offense has been committed; how the offense was committed; who committed it; where the offense was committed; when it was committed; and why it was committed. Taking of sworn statements of suspects and witnesses is also part of the investigation protocol. [4]

[3] An Act Establishing The Philippine National Police Under A Reorganized Department Of The Interior And Local Government, And For Other Purposes [Department of the Interior and Local Government Act of 1990] Republic Act No. 6975 (1990).
[4] Philippine National Police Criminal Investigation Manual (Revised), 2011.

Further, there are reporting requirements under existing laws which requires disclosure of information about particular medical conditions to specific government agencies, such as serious and less serious physical injuries[5] and suspected cases of child abuse or maltreatment.[6]

Nevertheless, while the DPA recognizes such mandate, the law is also categorical in stating that the processing of personal information must adhere to the principles of transparency, legitimate purpose and proportionality. Personal information must be processed for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection. It should also be processed in a way compatible with such declared, specified, and legitimate purposes only.

Law enforcement does not have a blanket authority to access medical records of patients in a hospital. These records may be released with patient's consent, or when being requested pursuant to a court order, subpoena or subpoena duces tecum, search warrants, or other administrative orders authorized by law.

Section 13(f) of the DPA does not provide law enforcement agencies unrestricted access to health information being kept in a hospital. Note that under the EU General Data Protection Regulation (GDPR),[7] "establishment, exercise or defense of legal claims" refers to processing of information in the context of seeking legal advice. This covers a range of activities, in the context of a criminal or administrative investigation, for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen, e.g. in anti-trust investigations. This also includes for the purpose of formal pre-trial discovery procedures in civil litigation and cover actions by the data controller to institute procedures for example commencing litigation or seeking approval of a merger.[8]

Section 13(f) should also be read in accordance with the 1987 Philippine Constitution, particularly Art. III, Section 2:

> "Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by

[5] P.D. 169, amended by E.O. No. 212, "Requiring Doctors, Hospitals, Clinics, etc. to Report Treatment of Physical Injuries" July 10, 1987

[6] The Child and Youth Welfare Code [Presidential Decree No. 603] Art. 166 (1974).

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016).

[8] Working Party of EU Data Protection Authorities, Guidelines on Article 49 of Regulation 2016/679 (February 6, 2018).

the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized."

Disclosure to the media

While hospitals may disclose personal information of patients to the police in relation to a criminal investigation as discussed above, there is no similar obligation for hospitals and other healthcare facilities to disclose personal information of patients to the media.

It should be noted that the DPA provides for the criteria for lawful processing of personal information and sensitive personal information in Section 12 and 13, respectively. Based on such criteria set in the law, personal and sensitive personal information of the patient can only be disclosed to the media when the patient gives his or her consent. The media does not have the legal mandate to compel hospitals and other health care facilities to disclose the information of their patients.

If there is an overriding public interest or public health issue to disclose patient information, the same may be taken into consideration in the evaluation of balancing patient privacy vis-a-vis the public's right to know. As a rule of thumb, whenever there is uncertainty as to whether the personal information should be disclosed or not, the PIC should strive to lean towards an interpretation that is mindful of the rights and interests of the individual about whom the personal information is processed.[9]

Policy for requests for personal information of patients

Considering the foregoing, it would be judicious on your part to develop a policy for requests for personal information and/or interviews from the police and the media. The policy may include guidelines on how the hospital can verify the veracity of the police investigation as well as confirm the occurrence of the alleged criminal act. This may be done through the presentation of a police blotter.[10] Also, an evaluation of the personal data required to be disclosed vis-à-vis its intended purpose should be done to ensure that it is relevant, necessary, adequate, and not excessive. [11]

The hospital and its personnel should not obstruct an investigation, but policies or procedures must be in place for balancing the legitimate

[9] Data Privacy Act of 2012, § 38.

[10] As a rule, all crime incidents must be recorded in the official police blotter. See: Philippine National Police Criminal Investigation Manual (Revised), 2011.

[11] See: Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).

interests of the State and the rights and freedoms of individuals, and for assuring the safety and security of all those in the hospital. The policies will have to consider the different instances when law enforcement authorities will be entering the hospital premises. For instance, the police may be bringing in a patient already under their custody, whether arrested for an offense or as inmate in a correctional facility. In dealing with these situations, the hospital will have security protocols in place, where presence of law enforcement may be deemed necessary. The hospital may itself also request for law enforcement assistance when the crime occurs in the hospital, or there is a threat to security within the hospital premises.

In other cases, law enforcement authorities may request to interview patients who are either suspected of committing a crime, are alleged victims, or are material witnesses. It is in these latter situations, where hospital policies should balance crime prevention, detection and investigation and that of the patient's rights, not only to data privacy, but to life and health. The hospital should be mindful that its first duty is to attend to patients in need of serious and emergency care, and for this purpose, access to patients may be limited if the same would put at risk the patient's life and health. For example, a patient who is unstable may require urgent medical interventions before any interview is allowed.

Lastly, it should be noted that as data subjects, the patients should be informed that they may be interviewed by the police in relation to investigations of crimes.[12] The police cannot compel an individual to agree to an interview, even if the individual is lawfully arrested.[13] The hospital should put in place policies to ensure that such interviews, where allowed, will be conducted in a manner that would protect the rights of other patients in the facility, and cause minimal disruption in the hospital operations. These may include providing a specific area where the interview will be conducted, and restricting access to other areas of the hospital. Where the situation presents unique considerations or challenges, part of the policy may be to promptly inform the Chief of the Hospital or designated officer of the situation.

When the one requesting for information is from the media, consent of patients should be obtained before disclosure thereof. It is suggested that any authorized disclosures to media be coursed through a hospital officer specifically designated to provide such information.

[12] See: Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (a).

[13] PHIL. CONST. art. III, § 12. (1) Any person under investigation for the commission of an offense shall have the right to be informed of his right to remain silent and to have competent and independent counsel preferably of his own choice. If the person cannot afford the services of counsel, he must be provided with one. These rights cannot be waived except in writing and in the presence of counsel.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-50

16 October 2018

[redacted]

Re: COLD CALLS AND EMAILS

Dear [redacted],

We write in response to your query received by the National Privacy Commission (NPC) via email. In your inquiry, you disclosed that majority of your activities as a salesman rely on making cold calls and sending cold emails to prospective clients. A potential customers' contact information is commonly obtained from publicly available sources, such as calling cards from events, exhibits and expos and the internet. Another method of acquiring contact information is through a speculation of email addresses based on established patterns.

You now request guidance on the legality of cold calls and emails in relation to Republic Act No. 10173,[1] otherwise known as the Data Privacy Act of 2012 (DPA), given that the targeted individuals have not specifically given their consent to the use of their personal information for marketing of your products or services.

Publicly Sourced Personal Data Protected under the DPA

Before all else, we note that "it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation."[2] In Section 4 of the DPA, the law specifies special cases where certain information may fall outside of its scope but only to the minimum extent necessary to achieve the specific purpose, function or activity.[3] As it is not recognized as a special case, publicly sourced personal data fall under protection of the DPA.

[1] 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).

[2] Office of the Privacy Commissioner for Personal Data, Hong Kong, Guidance Note - Guidance on Use of Personal Data Obtained from the Public Domain, August 2013, available at https://www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf (last accessed May 31, 2018).

[3] See Data Privacy Act of 2012, § 4.

Even though personal information of potential clients are obtained from publicly available sources, marketers employing such methods become personal information controllers (PICs) who must meet the requirements under the law. Marketers are bound by the provisions on criteria for lawful processing of personal, sensitive personal and privileged information provided by the DPA.

Direct Marketing as a Legitimate Interest

Calls and emails made directly to a potential customer without prior contact or lead, also known as cold calls and emails, are common direct marketing practices in the Philippines employed by companies, organizations and individuals for the offering or advertising of goods or services. Our own privacy law defines direct marketing as "communication by whatever means of any advertising or marketing material which is directed to particular individuals."[4]

Some activities involved in direct marketing, such as collection of potential clients' names, their contact details and email, business or home addresses, the storage of such information and the calling and emailing by sales representatives, involve the processing of personal data. Marketers, in their capacity as PICs, must then comply with the provisions of the law, including adherence to the data privacy principles of transparency, legitimate purpose and proportionality. The law further provides that a PIC must have a legitimate purpose for the processing of personal data, the criteria of which are specifically enumerated in Sections 12 and 13 thereof.[5]

In case the processing does not fall under any of the criteria enumerated under the law, consent given by the data subject should ideally be the basis of lawful processing of personal information for marketing purposes.[6]. For processing to be lawful, consent must have been given by the data subject prior to the collection, or if prior consent was not obtained, it should be given as soon as practicable and reasonable.[7]

Gathered from your inquiry, personal information was already processed upon collection of the prospective client's name and contact details. Thus, prior consent was not obtained. However, marketers may consider, with caution, legitimate interest as the basis of processing.

[4] Data Privacy Act of 2012, § 3 (d).
[5] Id. § § 12-13.
[6] Id. § 12 (a).
[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 21 (a) (2016).

In the assumption that only personal information and not sensitive personal information is involved, Section 12 (f) of the DPA may apply to this particular situation of direct marketing, **viz**:

> The processing is ***necessary for the purposes of the legitimate interests pursued by the personal information controller*** or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[8]

Furthermore, as our DPA is influenced by the 1995 EU Data Protection Directive and discussions on the EU General Data Protection Regulation (GDPR),[9] the latter's pronouncement on direct marketing holds significance. Recital 47 of the GDPR, in connection with Article 6(1)(f)[10] which is substantially the same as the above provision of the DPA, states: "... The processing of personal data for direct marketing purposes **may** be regarded as carried out for a legitimate interest."[11]

Thus, legitimate interests of a PIC may be considered as the lawful basis for making cold calls and emails to prospective clients. This notwithstanding, it cannot be said that direct marketing may **always** constitute legitimate interest.[12] Lawful processing of personal information on the ground of legitimate interest still depends on the particular circumstances.[13]

Legitimate Interests Three-part Test

Before a PIC may present legitimate interests as the basis for the processing of personal information for marketing activities, a three-part test must first be conducted.[14] The PIC must satisfy the following:

Purpose Test – is there a legitimate interest behind the processing?
Necessity Test – is the processing necessary for that purpose?
Balancing Test – is the legitimate interest overridden by the individual's interests, rights or freedoms?[15]

[8] Id. § 12 (f).
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016).
[10] GDPR, Article 6 (1)(f) provides:
(f) processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party except, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
[11] See GDPR, Recital 47.
[12] Information Commissioner's Office, UK, When can we rely on legitimate interests?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities (last accessed May 31, 2018).
[13] Id.
[14] Id.
[15] Information Commissioner's Office, UK, What is the 'legitimate interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ (last accessed May 31, 2018).

The DPA does not specifically provide which matters to consider in deciding whether a PIC's purpose counts as legitimate interest. Direct marketing activities which do not contravene any established law or ethical standards or practices may be considered as legitimate purpose.[16] The PIC must have a declared and specified purpose, not merely relying on vague or generic business interests, there must be some clear and specific benefit or outcome in mind.[17] As much as it can be argued that there are legitimate interests to be pursued, the PIC must next demonstrate that the processing is necessary and proportionate for the purposes of the identified legitimate interest.[18] Lastly, the PIC must determine whether the processing may be overridden by the fundamental rights and freedoms of the data subject and the impact of such processing on the data subject.[19]

In gauging whether interests of the individual may override the legitimate interests of the PIC, Recital 47 of the GDPR sheds some light thereon:

> At any rate the existence of a legitimate interest would need careful assessment including ***whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place***. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances ***where data subjects do not reasonably expect further processing***.[20]

Thus, the reasonable expectation of the data subject on the purpose for processing of his or her personal information at the time of its collection becomes a crucial consideration. Legitimate interests will likely be applicable where a PIC has a relevant and appropriate relationship with the data subject, such as when direct marketing is addressed to existing clients or employees.[21] In the absence of a pre-existing relationship, the PIC must demonstrate that the processing can be reasonably expected, particularly if the personal information was collected and obtained from a third party.[22]

In this situation, the questions for the sales representatives who may opt for cold calls and emails then are:

[16] Supra note 16.
[17] Id.
[18] Id.
[19] Id.
[20] GDPR, Recital 47.
[21] Information Commissioner's Office, UK, What is the importance of reasonable expectations?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/?template=pdf&patch=16 (last accessed August 14, 2018).
[22] Id.

1) What is the specific purpose or business objective that may be achieved by cold calls and emails?
2) Is this necessary and proportionate to his business objective?
3) Is there a possibility that the business interest of the marketer may override the individual interests and rights of the potential customer?
4) Did the data subject or potential customer expect further processing for a purpose different from that when his or her personal information was first collected or processed?
5) What, if any, is the impact of cold calls and emails on the individual or the data subject?

It may be argued that the individuals who gave their calling cards in events or expos may have expected calls or emails only from those individuals or organizations to whom they directly gave their contact information. For those individuals whose contact information are found online, they may have expected that their information will be used only for the purposes of such website or platform, e.g. job search and application. Further, such individuals may have reasonably expected that there will be no further processing of their information. Thus, a cold call or email from an entirely different organization or individual for marketing of different products or services may be considered an intrusion of their right to data privacy. Notwithstanding, each case should always be evaluated depending on the surrounding circumstances.

We wish to emphasize that legitimate interest is not intended to be a broad justification for all purposes assumed by PICs. The NPC, on its own determination, may evaluate whether legitimate interest is the proper basis for the specific processing, considering the interpretation clause under Section 38 of the DPA, where the law is liberally interpreted in a manner mindful of the rights and interests of the data subject.

Right to Information and Right to Object

Should the PIC be able to justify its legitimate interests, the DPA specifically provides that the data subject has the right to object and to withhold consent in relation to processing for direct marketing.[23]

In making cold calls and emails, marketers should be accountable, open and transparent in making said calls or emails. To achieve these, the potential customer must be apprised of the identity of the sales representative, the PIC or company he or she represents and the purpose

[23] Implementing Rules and Regulations of the Data Privacy Act of 2012, § 34 (b).

of the call and email.[24] The PIC, through their sales representatives, should also be able to communicate the source from which the contact details of potential customers were obtained, and the reasons for pursuing the direct marketing call. Direct marketers should also be able to give the individual the choice to allow or object to resume the call or the use of their personal data, and to assure that the data subject has the right to object at any given time should they wish to. Should the individual object at the initial contact done by the PIC, the PIC should immediately cease further direct marketing activities and any further kind of processing on the personal data of the individual, including storage and disclosure. The record on the individual's personal data should be destroyed.

Furthermore, sales representatives as accountable PICs should maintain appropriate measures which shall ensure the integrity and security of the personal data collected. Upon the conclusion of the purpose for processing, the collected personal information should be disposed of in accordance with the law. Finally, the PIC shall uphold the rights of the data subjects as provided by the DPA.[25]

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated. Please be advised that the NPC may issue further guidelines on this matter.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[24] Office of the Privacy Commissioner for Personal Data, Hong Kong, Guidance Note - New Guidance on Direct Marketing, January 2013, available at https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf (last accessed May 31, 2018).
[25] See Data Privacy Act of 2012, § 16.

ADVISORY OPINION
NO. 2018-51

16 October 2018

[redacted]

Re: VARIOUS CONCERNS REGARDING THE DATA PRIVACY ACT

Dear [redacted],

We write in response to your request concerning various inquiries and clarifications regarding the Data Privacy Act of 2012[1] (DPA), particularly the following:

1. Are there any unconstitutional provisions in the DPA?

The DPA is presumed constitutional unless otherwise declared by the Supreme Court of the Philippines.

Statutory acts of Congress are accorded with the presumption of validity. The presumption is that the legislature intended to enact a valid, sensible and just law which only does what is needed to achieve the specific purpose of the law. Every presumption should be indulged in favor of constitutionality and the burden of proof is on the party alleging that there is a clear and unequivocal breach of the Constitution.[2]

2. How does NPC legally define Personal Information?

Section 3(g) of the DPA clearly defines p*ersonal information* as 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.

[1] 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).
[2] Lawyers Against Monopoly and Poverty (LAMP), et al. v. The Secretary of Budget and Management, et al., 686 Phil. 357, 372 (2012), citing Farinas v. The Executive Secretary, 463 Phil. 179, 197 (2003).

3. How does NPC legally define Sensitive Personal Information? What is the difference between Personal Information and Sensitive Personal Information?

Section 3 (l) of the Act enumerates what are considered as **Sensitive Personal Information**, to wit:

> (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 person, 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 not limited to, social security numbers, previous or cm-rent 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.

The DPA provides for different sets of criteria for lawful processing of personal information and sensitive personal information.[3] In Section 12 of the DPA, processing of personal information is allowed only if not prohibited by law and when at least one of the conditions enumerated in the provision exists. On the other hand, Section 13 states that generally, processing of sensitive personal information and privileged information is prohibited, unless the basis for processing is among the cases indicated.

Moreover, the law imposes higher penalties for violations involving sensitive personal information.

4. How does NPC legally define Privileged Communication?

The Commission adopts the definition of the Rules of Court[4] and other pertinent laws on what constitutes privileged communication.[5]

5. If the "data processor" has never had any data protection officer, what are the requirements and costs?

[3] Republic Act No. 10173, § 12 and 13.
[4] See: Revised Rules on Evidence, Rule 130, §24.
[5] Republic Act No. 10173, § 3(k).

A Data Protection Officer (DPO) should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security and/or data protection needs. Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.

You may also refer to NPC Advisory 2017-01 for further guidance on the designation of a DPO.

6. If the "data processor" has never had any data protection officer what are the penalties?

The designation of a DPO is a means to comply with Section 21(c) of the Data Privacy Act. A violation of the Data Privacy Act and any other issuances of the Commission can lead to compliance orders and other enforcement actions. The failure of the organization to appoint or designate a DPO will be taken into consideration in the event of an investigation or a compliance check. In the event of a breach, the lack of a DPO may be considered evidence of negligence.

7. What is the penalty if personal data is not processed fairly and lawfully by failing to update address, phone number, email, name in SSS/PhilHealth/Pag-Ibig/BIR, as stated in Section 11 (b) and (c)?

For the most part, the duty to update lies with the data subject since they are the ones who will know of any changes in their personal information. All PICs need to do is to give them an opportunity and a mechanism to update their information.

Fair and lawful processing of personal information entails adherence to the principles of transparency, legitimate purpose and proportionality.[6]

First, the personal information controller must inform the data subject on the nature, purpose and extent of processing of his or her personal data, and the rights as data subjects and how these rights can be exercised, among other details to be disclosed.[7]

Second, the processing activity must be based on a legitimate, declared

6 Republic Act No. 10173, §11.
7 Implementing Rules and Regulations (IRR) of Republic Act No. 10173, known as the "Data Privacy Act of 2012," §18 (a).

and specified purpose, which is not contrary to law, morals or public policy.[8] This will serve as the legal basis for processing of personal data.

Lastly, the personal information controller shall only process adequate, relevant, suitable, and necessary information to achieve or fulfill the declared purpose of processing.[9]

Failure to update personal data may not necessarily amount to any of the acts punishable under the DPA, especially if such is due to the fault of or attributable to the data subject. Nevertheless, the DPA provides for the right of data subjects to reasonable access to their personal information, the right to dispute inaccuracy or error in their personal information, and the right to have them rectified, supplemented, destroyed or their further processing restricted.

In the event that the data subject has exercised the right to rectify the errors to reflect accurate information and the personal information controller fails to recognize such right, the data subject has the right to be indemnified for any damages sustained due to the inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of their personal information. Nonetheless, damages may only be imposed upon the PIC's refusal to correct the personal data after a reasonable request from the data subject.[10]

Pertinent laws and regulations on the Social Security System (SSS), Philippine Health Insurance Corporation (PHIC), Home Development Mutual Fund (Pag-IBIG), and the Bureau of Internal Revenue (BIR) will likewise apply, as the case may be.

8. Does refusing access to the employee 201 file a violation of DPA? The employee 201 is a logbook of an employee's records and may include detrimental information written by the employer without the knowledge of the employee.

The DPA does not prevent employers from collecting, maintaining, and using employment records. However, employers should also strive to strike a balance between the need to keep records of their employees and the employees' right to access their personal data. Section 16(c) provides for the right of data subjects to reasonable access to the following:

[8] Id., §18 (b).
[9] Id., §18 (c).
[10] Republic Act No. 10173, §16.

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller.

Nevertheless, the right to access only refers to personal data and related information as enumerated above and not to all kinds of employment records.

9. Please clarify or provide basis about "the corporation is a judicial entity and has no right against self-incrimination?"

Being a juridical body, a corporation does not have a right against self-incrimination. In the case of compliance with the DPA, this means that any submission on data processing systems should not be considered as an issue of self-incrimination but as a submission to a regulatory body tasked with administering and implementing the law.[11]

The basis for this can be found in the case of **Bataan Shipyard & Engineering Co., Inc. v. Presidential Commission on Good Government,**12 where the Supreme Court ruled that while an individual may lawfully refuse to answer incriminating questions unless protected by an immunity statute, it does not follow that a corporation, vested with special privileges and franchises, may refuse to show its hand when charged with an abuse of such privileges. Citing the case of Wilson v. United States, 55 Law Ed., 771, 780., the court reiterated that since the corporation is created for the benefit of the public, the special privileges and franchise granted to it are subject to the laws of the land and limited by its charter. Thus, the state can inquire at any time whether the corporation is operating accordingly or is exceeding its powers.

[11] NPC Advisory Opinion No. 2017-64
[12] GR No. L-75885, May 27, 1987.

10. "Can an employee request a copy of the Data Sharing Agreements (DSA) from their employers?"

Yes, the employee can request for a copy of the DSA from their employers or the personal information controller, if the DSA involves their personal data, pursuant to their right to be informed of the personal information controllers processing their data and the right to access as data subjects.[13]

"Scenario #1: According to a "witness" named Patricia claims Rody stole the money from the cashier's desk but Rody was not there. Unfortunately, there is no one willing to prove Rody that he was not at the shop but there are CCTV cameras aimed at recording the cashier's desk. So whoever stole the money, the CCTV records would reveal who it is. However, the shop will not give nor show the CCTV because she is the owner and wants Rody kicked out. Can Rody request the CCTV footage through the NPC since he is the data subject?"

Considering that the CCTV camera is placed and strategically aimed at the cashier, the main purpose of installing the CCTV camera may be to monitor financial operations. Whoever then is stationed at the cashier is the data subject with the right to reasonable access[14] to the particular footage involving him or her. As his image was not captured by the CCTV, Rody is not the data subject since there is no processing of his personal information in the given scenario. Therefore, he cannot invoke the right to access under the DPA.

Nonetheless, Rody may request a copy of the CCTV footage as evidence to establish his defense before the investigation committee of the organization. However, request should be lodged with the personal information controller, the establishment, who has custody of the footage, and not with the NPC.

The DPA defines a data subject as an individual whose personal information is being processed.[15]

Processing involves a wide array of activities performed upon personal information, including but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[16] Based on the enumeration, the recording of the operations in the establishment

[13] Republic Act No. 10173, §16(c).
[14] Id., §16(c).
[15] Id., § 3(c).
[16] Id., § 3(j).

or property, capturing therewith images of customers or employees, is considered as a processing activity.

The closed-circuit television (CCTV) is a camera surveillance system that captures images of individuals or information relating to individuals.[17] If the camera surveillance footage is of sufficient quality, in such a way that the identity of an individual can be reasonably ascertained, it can be potentially classified as personal information, thereby, the provisions of the DPA will apply.[18]

The establishment, as the personal information controller, has the duty to implement security policies and guidelines on how footages can be viewed, or acquired and those authorized to access, when data can be shared or transferred and the corresponding retention period. The data subjects must be informed, through a privacy notice, that the establishment is being monitored by a CCTV camera.[19]

11. "Scenario #2: A lot of people have been candidly and secretly photographed then posted online. They may appear harmless but the risks of being accused of something because a "social media" site has your picture on the profile shown and others think it was you. What are possible actions to seek its removal and identify the perpetrators."

The act in the given scenario may be considered as unauthorized processing,[20] depending on circumstances of the case. The DPA penalizes persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law. This is subject to other provisions of the DPA. For instance, an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs is not considered a personal information controller as defined under the DPA.[21] The DPA also treats as special cases processing for journalistic, artistic, literary or research purposes.[22]

In cases like these, the affected data subject is entitled to suspend, withdraw or order the blocking, removal or destruction of his or her personal information upon discovery and substantial proof that the personal

[17] Office of the Privacy Commissioner, New Zealand, Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations (2009), , available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf, last accessed on 25 April 2018.
[18] Office of the Information Commissioner Queensland, Camera Surveillance and Privacy (2009), available at https://www.oic.qld.gov.au/__data/assets/pdf_file/0006/7656/Camera-Surveillance-and-Privacy.pdf, last accessed on 25 April 2018.
[19] IRR of Republic Act No. 10173, § 18.
[20] Republic Act No. 10173, § 25.
[21] Id., § 3(h [2]).
[22] Id., § 4(d).

information is unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.[23]

The provisions of the Anti-Photo and Video Voyeurism Act of 2009[24] or the Cybercrime Prevention Act of 2012[25] may also apply as the case may be. Special divisions of law enforcement may assist in identifying perpetrators.

12. "Scenario #3: Does the media or anyone who makes inquiries need to request consent of an interviewee before they can interview? Some of the ambush interviews tend to be rude and can come in at a wrong time, so does the law protect this? Does the law protect personal space in the same way as hands-off to private parts?"

Section 4(d) of the DPA provides for the non-applicability of the law on personal data processed for journalistic, artistic, literary or research purposes. The Implementing Rules and Regulations (IRR) explain that this non-applicability is made "in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations."[26] Note, however, that the non-applicability of the DPA is only to the minimum extent necessary to achieve the specific purpose, function, or activity concerned.[27]

Stated otherwise, the exemption is not a carte blanche authorization that journalists can conveniently present to compel potential sources of information to turn over or disclose data under their custody. After all, public disclosure of data remains subject to a range of policies, including internal ones maintained by organizations, and other laws, as enacted or issued by the appropriate legislating authority. Thus, members of the media cannot compel a person to grant an interview without the latter's consent.

As to the protection of physical personal space, it is not covered by the DPA. The DPA relates to informational privacy and protection of personal information. In any case, the right to privacy is constitutionally protected and accorded recognition independent of its identification with liberty. There are existing laws and regulations that protect the right to personal space.

---

[23] Id., § 16 (e).
[24] An Act Defining and Penalizing the Crime of Photo and Video Voyeurism, Prescribing Penalties Therefor, and for Other Purposes [ANTI-PHOTO AND VIDEO VOYEURISM ACT OF 2009], Republic Act No. 9995 (2010).
[25] An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties for Other Purposes [CYBERCRIME PREVENTION ACT OF 2012], Republic Act No. 10175 (2012).
[26] IRR, §5(b).
[27] Id.

13. "What happens if data subjects are not notified or informed of their rights under Section 16 of the DPA? How much do we have to pay to file a complaint or request an advisory opinion from the NPC?"

The personal information controller or personal information processor shall uphold the rights of data subjects and adhere to general data privacy principles and the requirements of lawful processing. Thus, when a data subject thinks that an entity is processing his or her personal data in violation of his or her right as data subject, he or she may seek redress with the organization for appropriate action on the same or file a complaint with the Commission.[28]

Further, the data subject may be indemnified for any damages sustained due to the inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.[29]

Currently, the Commission does not prescribe a fee for filing of complaints and request for advisory opinions.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

[28] For further guidance, see: NPC Circular 16-04 (December 15, 2016).
[29] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34(f).

ADVISORY OPINION
NO. 2018-052

16 August 2018

[redacted]

Re: CHED MEMORANDUM ORDER NO. 3, SERIES OF 2012

Dear [redacted],

We write in response to your letter to the National Privacy Commission (NPC), requesting comments on the authority of the Commission on Higher Education (CHED) to collect data for its "monitoring and validation activities" under CHED Memorandum Order No. 3, series of 2012, "Enhanced Policies, Guidelines and Procedures Governing Increases in Tuition and Other School Fees, Introduction of New Fees, and for Other Purposes" (CMO No. 03) in relation to the Data Privacy Act of 2012 (DPA).[1] You have likewise provided us the following documents:

1. CMO No. 08, s. 2012 – "Amendment on CMO No. 03, s. 2012;"
2. CHED Regional Offices' Reportorial Requirements for the Applications to Increase in Tuition and Other School Fees (TOSF); and
3. Prescribed templates as annexes to the proposed revision of CMO No. 03, s. 2012:
    a. Data requirement for the application to increase in TOSF;
    b. Report on the Actual Utilization of Incremental Proceeds in TOSF; and
    c. Monitoring and Evaluation Framework.

We understand that the CHED monitors compliance of the private HEIs with the prescribed percentage distribution of the incremental proceeds from the increase in TOSF. HEIs are required to use seventy percent (70%) of the incremental proceeds for the benefit of teaching and non-

[1] 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).

teaching personnel and other staff, except those who are principal stockholders of the HEI.[2]
HEIs then submit their payrolls, payslips, acknowledgement of increase remittances, notice of salary adjustments, faculty and staff benefits, and other relevant documents to substantiate this requirement.

You stated that the monitoring and validation activities of the CHED is being challenged by private Higher Education Institutions (HEIs) on the basis of the DPA. The CHED now seeks clarification on its authority to collect data for its mandatory reportorial requirement under CMO No. 03 vis-à-vis the DPA.

Lawful processing of personal data

The CHED, as a personal information controller (PIC), is allowed to process personal data taking into consideration the provisions of the DPA on upholding the rights of data subjects, adherence to the principles of transparency, legitimate purpose and proportionality, and implementing reasonable and appropriate organizational, physical and technical security measures intended for the protection of personal data.

The CHED has promulgated CMO No. 03 and its amendment, CMO No. 08, to govern its monitoring and validation activities and prescribed guidelines for the reportorial requirements relevant to TOSF. Under these regulations, CHED collects both personal information[3] and sensitive personal information[4] (collectively, personal data) from HEIs.

This processing is necessary in order for CHED to fulfill its mandate under various laws, including Batas Pambansa Blg. 232[5] (Education Act of 1982) and Republic Act No. 77226 (Higher Education Act of 1994). As a regulatory agency, CHED is authorized to monitor and validate the utilization of the proceeds of TOSF and may collect relevant documentation for this purpose. In these cases, CHED should ensure that its regulatory enactments guarantee the protection of personal data.

[2] CMO No. 03, § 7.2.2 and 7.2.3, as amended by CMO No. 08.
[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 3 (l): 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;
[4] Id. § 3 (t): 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.
[5] An Act Providing for the Establishment and Maintenance of an Integrated System of Education [Education Act of 1982], Batas Pambansa Blg. 232 (1982).
[6] An Act Creating the Commission on Higher Education, Appropriating Funds Therefor and for Other Purposes [Higher Education Act of 1994], Republic Act No. 7722 (1994).

Proportionality

The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[7] Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[8]

While the CHED may require the submission of pertinent documentation necessary to verify the utilization of the incremental proceeds from the increase in TOSF, it is worth noting that the CHED may consider accepting aggregated data, i.e. information from an HEI's audited financial statements on the revenues vis-à-vis amount of salaries and benefits given to its personnel and other staff, other forms of reports and certifications from an HEI's responsible officers as to the utilization, instead of requiring the submission of documents containing personal data of the employees.

However, should the CHED still require the submission of sample payrolls, payslips, acknowledgement of increase remittances, notice of salary adjustments, among others, it may opt to accept documents where personal data unrelated to the purpose of the validation is duly redacted.

Security Measures

As a PIC, CHED should implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. CHED should put in place policies and procedures on access controls, such that access shall be limited to only authorized personnel and personal data shall not be further processed except upon instructions or as authorized by law or policy.[9] In addition, the security measures should ensure to maintain the availability, integrity, and confidentiality of personal data, protect the same from any accidental or unlawful destruction, alteration, disclosure and unlawful processing.[10]

We trust that the CHED is well aware of its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, which requires all government agencies engaged in the processing of personal data to observe the following duties and responsibilities:

[7] IRR of the Data Privacy Act of 2012, § 18 (c).
[8] Ibid.
[9] Id. § 25.
[10] Ibid.

A. through its head of agency, designate a Data Protection Officer;

B. conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data, **Provided**, that such assessment shall be updated as necessary;

C. create privacy and data protection policies, taking into account the privacy impact assessments, as well as Sections 25 to 29 of the IRR;

D. conduct a mandatory, agency-wide training on privacy and data protection policies once a year: **Provided**, that a similar training shall be provided during all agency personnel orientations.

E. register its data processing systems with the Commission in cases where processing involves personal data of at least one thousand (1,000) individuals, taking into account Sections 46 to 49 of the IRR;

F. cooperate with the Commission when the agency's privacy and data protection policies are subjected to review and assessment, in terms of their compliance with the requirements of the Act, its IRR, and all issuances by the Commission.[11]

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated. Please be advised that the Commission may issue further guidelines on this matter.

For your information.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[11] NPC Circular No. 16-01 dated 10 October 2016, §4.

ADVISORY OPINION
NO. 2018-053

26 November 2018

[redacted]

Re: PHOTOGRAPHS AND CCTV FOOTAGES IN HOSPITALS

Dear [redacted],

We write in response to your query on the applicability of the Data Privacy Act of 2012 (DPA)[1] to the following:

a. taking of photographs of hospital staff and hospital premises by patient's family members;
b. clinical photographs; and
c. closed circuit television (CCTV) footages.

Photographs of hospital staff, doctors, and hospital premises

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.[2] Accordingly, the image of an identifiable individual captured in a photograph or video is personal information about the individual, and thus, covered by the DPA.

Given that processing of personal information, including photographs, must be in accordance with law, pictures of hospital staff and doctors can only be lawfully taken and processed when at least one of the following conditions set forth in Section 12 of the DPA exists:

[1] 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).
[2] Data Privacy Act of 2012, § 20 (c).

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs is not considered a personal information controller as defined under the law.[3] Where an individual is taking photographs for personal affairs, he or she must still be mindful of respecting rights to privacy of others.

As to photographs of hospital premises, the DPA will not apply, as long as the photo does not capture other individuals or data subjects within the premises where they are identifiable. This does not mean that other laws, regulations and generally accepted hospital standards will not apply.

CCTV images and footage; clinical photographs

Same as photographs of hospital staff and doctors, CCTV images and footage are considered personal information inasmuch as it contains an image of an identifiable individual. Hence, the criteria for lawful

[3] Data Privacy Act of 2012, § 3 (h) (2).

processing under Section 12 of the DPA would also apply.

Clinical photographs, on the other hand, are sensitive personal information since they necessarily contain the health information of patients.[4] Thus, processing thereof is prohibited except in the following cases:

> (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
>
> (b) The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
>
> (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;
>
> (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
>
> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

[4] Id. § 3 (l) (2).

Based on the provision above, if clinical photographs are taken by doctors, nurses, and other healthcare professionals for medical treatment purposes, it is allowed under the DPA, provided that an adequate level of protection of the personal data is ensured.

Policy regarding photographs and CCTV

Considering the foregoing, it is recommended that the hospital craft and implement its own policy about the collection and processing of photographs and CCTV, including specific guidelines or instances when taking of photographs is allowed and security measures as to the use and transmission of clinical photographs.

Furthermore, every personal information controller shall recognize the right of data subjects to be informed and notified[5] of the processing activities involving their personal data. The hospital must post a privacy notice on conspicuous areas to apprise the data subjects that the hospital premises or particular areas that are under surveillance of CCTVs.

This notification should sufficiently explain the policy on CCTV and the rights of data subjects. Specifically, it must be able to elaborate on the data subject's right to access CCTV footage and images, and/or request for copies, upon approval of request and with appropriate masking of the personal data of other individuals, where applicable.[6]

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

[5] Data Privacy Act of 2012, § 16 (a) and (b).
[6] Id. § 16 (c).

ADVISORY OPINION
NO. 2018-054

04 December 2018

[redacted]

[redacted]

Re: PATIENT REGISTRY, RESEARCH, AND THE DATA PRIVACY ACT OF 2012

Dear [redacted],

We write in response to your letters which sought to clarify the development and use of health information registries, particularly patient registries, for research studies.

Specifically for [redacted] query, it sought advice regarding the linkage of cancer incidence data of the Department of Health (DOH) - Rizal Cancer Registry and Philippine Cancer Society (PCS) - Manila Cancer Registry (Registries) with mortality data from the Philippine Statistics Authority (PSA), and the possibility of an exemption or a special policy coverage under Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations[2] (IRR), and relevant issuances of the National Privacy Commission (NPC).

DPA and research

Section 4 of the Data Privacy Act enumerates categories of information outside the scope of the law. This includes processing of personal information for research purposes.[3] This exemption, however, is not absolute, but only to the minimum extent necessary to achieve the

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173.
[3] Data Privacy Act of 2012, §4.

specific purpose, function, or activity,[4] and subject to the requirements of applicable laws, regulations, or ethical standards.[5]

First, research purpose is strictly interpreted to refer to processing intended for a public benefit.[6] Maintaining a registry for research purpose falls within the special cases recognized by the DPA.

Second, the processing will be exempted only to the extent necessary. Personal information controllers[7] (PICs) and personal information processors[8] (PIPs) engaged in research which involves sensitive personal information are expected to comply with their obligations under the DPA on the implementation of organizational, technical, and physical security measures to ensure the protection of personal data against accidental or unlawful destruction, alteration, disclosure, or unlawful processing.[9] PICs are also responsible for personal information under its control or custody, including those transferred or shared with third parties.[10]

Third, the flexibility for research purposes will only apply in so far as it is consistent with ethical and legal standards. This means that there are instances when the consent requirements for research may be waived if such waiver is consistent with legal and ethical principles. Likewise, the rights of data subjects may also be limited where such limitation is necessary to maintain research integrity.

One way of demonstrating adherence to ethical standards is by seeking the approval of a duly recognized Research Ethics Committee (REC)/ Internal Review Board (IRB)/Ethics Board (EB)[11] for the research protocol, including the waiver of the consent requirement for research purpose.

We understand that the Registries - Rizal Cancer Registry and Manila Cancer Registry – are maintained by the government and a private institution, respectively. We assume that sensitive personal information in these Registries have been collected and processed pursuant to a statutory mandate in the case of the DOH, and consent of data subjects, in the case of the PCS. Without consent from data subjects, the burden is on PCS to demonstrate that the processing of sensitive personal information without consent is consistent with legal and ethical standards.

---

[4] Id, §5.
[5] Id., §5(c).
[6] Supra note 13.
[7] Id. § 3 (h).
[8] Id. § 3 (i).
[9] Id, §20.
[10] Id, §21.
[11] Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical Guidelines, National Ethical Guidelines for Health and Health Related Research 15 (2017).

While maintaining a registry for research purposes may be permitted under the DPA, linkages with the PSA database may be subject to other laws allowing disclosure of information to the public.

The PSA is mandated to ensure confidentiality of all primary data that they retain.[12] Consequently, the agency may only release the aggregated information in a summary form.[13] Further, Republic Act 10625,[14] otherwise known as the Philippine Statistical Act of 2013, and its implementing rules and regulations, prohibit the agency from disclosing information that may lead to any person's identity, unless otherwise mandated by another law. Under the DPA, the criteria for lawful processing of sensitive personal information are:

a. The data subject has given his or her consent;
b. The processing of the same is provided for by existing laws and regulations;
c. The processing is necessary to protect the life and health of the data subject or another person;
d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, that the sensitive personal information are not transferred to third parties: Provided, finally, that consent of the data subject was obtained prior to processing;
e. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
f. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

Where one of the criteria provided in the DPA is met, sensitive personal information may be processed and shared. Note also that data sharing between government agencies for the purpose of a public function

[12] An Act to Create a Bureau of the Census and Statistics to Consolidate Statistical Activities of the Government therein [BUREAU OF CENSUS AND STATISTICS], Commonwealth Act 591 (1940) §4.
[13] Id.
[14] An Act Reorganizing The Philippine Statistical System, Repealing For The Purpose Executive Order Numbered One Hundred Twenty-One, Entitled "Reorganizing And Strengthening The Philippine Statistical System And For Other Purposes" [PHILIPPINE STATISTICAL ACT OF 2013], Republic Act No. 10625 (2013).

or provision of a public service should be covered by a data sharing agreement. Please refer to NPC Circular No. 16-02 - Data Sharing Agreements Involving Government Agencies - for additional details.

In view of the foregoing, it is best to consult with the PSA Legal Service and clarify if it is possible for the DOH and the PCS to provide PSA with a list of specific individuals from their respective databases and for the latter to match this with its mortality database, i.e. provide a "Yes" or "No" answer as to the status of those individuals, taking into consideration the provisions of NPC Circulars No. 2016-01 (Security of Personal Data in Government Agencies) and 2016-02 (Data Sharing Agreements Involving Government Agencies)

This opinion is provided based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-056

05 October 2018

[redacted]

[redacted]

[redacted]

Re: WEB-BASED ACCREDITATION SYSTEM FOR HOSPITALS

Dear [redacted],

We write in response to your request for an advisory opinion regarding the Web-based Census and Accreditation System (WebCAS) facility, a system that uses personal information of patients submitted by institutions for purpose of their accreditation as pulmonary fellowship training hospitals. You requested for clarification on how the Data Privacy Act of 2012 (DPA)[1] applies to your arrangement with various hospitals, particularly on the following:

1. Whether the transfer of patient data for accreditation or proof of fulfilment is allowed by the Data Privacy Act of 2012 (DPA);
2. Whether consent from patients is required for inclusion of their personal information in the census or whether this is considered quality management where consent may not be required; and
3. Whether de-identification allows retaining hospital number, age and gender of patients?

[1] 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).

Lawful processing of sensitive personal information

A patient's health information is considered as sensitive personal information under the Data Privacy Act. The DPA views information about a person's health as posing a significant risk to data subjects in case of unlawful or unauthorized processing due to its sensitive nature. In general, the processing[2] of sensitive personal and privileged information are prohibited unless one of the conditions stipulated in Section 13 of the DPA is satisfied. Thus, the transfer of patient data from a hospital to the Philippine College of Chest Physicians (PCCP), and its processing in the WebCAS for accreditation purposes, should rely on one of the conditions for lawful processing under Section 13 of the DPA.

Sensitive personal information may be lawfully processed if "the data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing."[3] Section 13 also provides conditions where consent may not be required for lawful processing. This includes processing for medical treatment purpose, or when necessary to protect the life and health of the data subject or another person and the data subject is unable to physically or legally express consent.

The use of the patient's health information for accreditation and training purpose requires consent from patients. A consent guide is available in the NPC Privacy Toolkit accessible at the NPC website.[4]

The processing in this context is not in the nature of a quality management system where the processing is generally internal to the hospital. In this case, the processing involves the transfer of sensitive personal information under control of the hospital to PCCP, and further processing of the same information by the latter. Second, the PCCP does not have a direct relationship with the patient. Where the hospital processes patient data for its own quality management for the purpose of generating statistical data, the hospital is processing personal information under its control and custody. The DPA recognizes that personal information collected for other purposes may be processed for historical, statistical or scientific purposes.[5] This is seen to be compatible with the primary purpose. On the other hand, the PCCP's collection and access to the health information falls outside a patient's reasonable

[2] Data Privacy Act of 2012, § 3 Definition of terms, (j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
[3] Id., §13(a)
[4] See National Privacy Commission, Toolkit, available at https://privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf (last accessed Oct. 5, 2018).
[5] Id., §11(f)

expectation. The patient, as the data subject, should be fully aware of the purpose, extent, and risks of the said processing.

De-Identification

Alternatively, the PCCP may consider obtaining only de-identified personal data from hospitals. Where statistical or aggregated data has already been generated by the hospital, the information will no longer be considered personal information, and may already be used for various purposes.

De-identification may entail the removal of the following personal information:[6]

- Name
- All geographic subdivisions, including street address, city, ZIP Code
- All elements of dates (except year) for dates that are directly related to an individual, including birth, date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet protocol (IP) numbers
- Medical records numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying numbers, characters, or code
- Certificate/license numbers

The purpose of de-identification is to remove identifiers so that the remaining information no longer relates to an identified or identifiable person. The "de-identification" being contemplated in this case, where

[6] U.S. Department of Health & Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale (last accessed 30 July 2018).

data about hospital number, age and gender are retained, is more appropriately a process of pseudonymization. The inclusion of the hospital number of patients makes it possible to still link the data set to a particular patient, and thus the information cannot be considered as de-identified. Pseudonymized data is still personal information subject to the provisions of the DPA. The benefit of using pseudonymized data is that it demonstrates proportionality in data processing, where the risks to the data subject are decreased.

In all cases, the processing of the said personal data shall be subject to the compliance with the requirements of the DPA, IRR, NPC issuances and other relevant rules and regulations. There should be adherence to principles transparency, legitimate purpose and proportionality. Patients should be informed about their rights, and how they may exercise such rights. Personal information controllers, such as the hospitals and PCCP, should also implement reasonable and appropriate organizational, technical and physical security measures intended for the protection of personal information against any accidental or unlawful disclosure, as well as against any other unlawful processing.

This advisory opinion is rendered based on the questions and information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts. Note that the proposed Memorandum of Agreement between PCCP and the participating training institutions has not been reviewed for purposes of this advisory opinion.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-057

20 September 2018

[redacted]

Re: OUTSOURCING AGREEMENT

Dear [redacted],

We write in response to your query received by the National Privacy Commission (NPC) via email. You stated that Automatic Data Processing (ADP) is a human capital management solutions company based in the United States. It has presence in the Philippines through ADP (Philippines) Inc. which provides payroll services to Philippine clients. You seek advice and clarification regarding Section 44 of the Implementing Rules and Regulations (IRR)[1] of Republic Act No. 10173,[2] otherwise known as the Data Privacy Act of 2012 (DPA).

We provide the following clarifications:

1. On Section 44 of the IRR, you inquire if there are any restrictions on modifying the terms used in the same provision for data outsourcing agreements.

We confirm that Section 44 of the IRR on Agreements for Outsourcing does not prevent the parties to the contract from modifying the same if the required stipulations laid down in Section 44(b) are clearly set out therein. The parties may add or provide other terms and conditions in the outsourcing agreement.

2. On Section 44 (a), particularly on the requirement to indicate the geographical location of processing in relation to your multinational clients with a global presence which require multiple

[1] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
[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).

data hosting locations, you seek advice on whether your current approach, i.e. providing clients with an indicative list of countries where their data will be hosted and accessed, obtaining a blanket approval for cross border data transfers in the contract and communicate changes, if any, on a set frequency, either annually, bi-annually or quarterly, meets the requirement under the law.

It is sufficient that the agreement states the indicative list of countries where personal data of clients that require multiple data hosting locations will be processed. We further note that in case there may be changes, the same should be communicated to the parties to the contract. In the case of cross-border data transfers, the applicable laws of the different jurisdictions and international agreements, if any, will apply.

The DPA provides for no restrictions on cross-border data transfers from a personal information controller to a personal information processor located in another jurisdiction so long as the PIC ensures that proper safeguards are in place to ensure the confidentiality, integrity and availability of the personal data processed, and prevent its use for unauthorized purposes as well as comply with the requirements of the DPA, the IRR and other issuances of the Commission.

3. On Section 44 (b)(1) and (4) on the processing by another processor or sub-contractor, you inquired whether including a blanket approval in the contract for (a) cross border data transfers and (b) engaging another processor/sub-contractor/vendor, subject to the same confidentiality, security and privacy provisions, meet the requirement of the IRR? Would proactively communicating cross-border data transfers/processor changes to clients prior to implementing said changes and providing a mechanism to object to the change satisfy the requirement in IRR?

The personal information controller should already be apprised of the possible jurisdictions where personal data will be transferred to as well as the possible engagement of another processor, sub-contractor or vendor if the same can be already identified. The proposed communication of changes on cross-border transfers/processors or sub-contractors should, at the very least, provide a mechanism that gives the personal information controller a sufficient period of time to object before the proposed changes are implemented in order to comply with the requirements of the IRR. As mentioned above, kindly note that stipulations on cross-border data transfers are always subject to the laws and regulations of the particular jurisdictions involved.

4. On Section 44 (b)(7) on retention of data, you stated that from a technology standpoint, data on archival media/backup tapes cannot be disturbed or destroyed. You seek clarification on whether archives and backup tapes may be exempt from the requirement under the DPA for the deletion of existing copies.

No, archival media or backup tapes are not exempt from the law. While personal data may be retained for a certain period pursuant to legitimate business purposes, such purpose must be consistent with standards followed by the applicable industry.[3] Taking into consideration the technical challenges, companies must start considering strategies on how to make data erasure possible, or how to put in place measures to prevent further processing of data on archival media/backup tapes. The DPA provides that personal data shall not be retained longer than necessary.[4] Where data is being retained, PICs should document its justification and ensure that data subjects are fully notified of such retention, the purpose and other relevant information.

5. On Section 44 (b)(8) on the requirement to make available to the personal information controller all information necessary to allow for and contribute to audits by said PIC or another auditor mandated by the PIC, you inquire whether there is further guidance on said provision; whether it is possible to restrict such an audit to select situations which require an audit and establish terms and conditions that would require the audit to be performed in a manner that would not compromise another client's data or the vendor's internal protocols; and whether it is possible to require the parties to mutually agree on the auditor.

The purpose of the provision is to allow the personal information controller to have access to necessary information in the hands of the processor in case of audits and inspections. The audits and inspections contemplated in the provision are not limited to those conducted by the personal information controller itself or another auditor mandated by the latter, but also those required by the DPA, its IRR and pertinent issuances of the NPC.

The parties may include appropriate stipulations on the conduct of audit in certain circumstances, as well as those which would require audits to be performed in a manner that would not compromise another client's data or the PIP's internal protocols, and even the requirement that parties shall mutually agree on the auditor, if feasible.

[3] Id., § 19 (d)(1)(c).
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (d).

All of these are subject to the precept that contracting parties may establish such stipulations, clauses, terms and conditions as they may deem convenient, provided they are not contrary to law, morals, good customs, public order, or public policy.[5]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[5] An Act To Ordain And Institute The Civil Code Of The Philippines [THE CIVIL CODE OF THE PHILIPPINES] Republic Act. No. 386 (1949), Art. 1306.

ADVISORY OPINION
NO. 2018-058

26 October 2018

[redacted]

Re: AYALA REWARDS CIRCLE

Dear [redacted],

We write in response to your request for guidance on the applicable rules and guidelines that have been issued on the requirement for obtaining consent relative to the loyalty programs offered to members of the Ayala Group Club, Inc., under the name and style Ayala Rewards Circle (ARC).

We understand that some queries were received by ARC from its members seeking clarification on the conditions necessitating an organization to reobtain consent, in lieu of a prior notice where changes have been made to the terms and conditions of the program, particularly where such changes are merely formal in nature and intended for the data subjects' better comprehension of ARC's processing activities.

ARC is of the opinion that the consent of the individual members need not be obtained anew in relation to the revised terms and conditions.

Ayala Rewards Circle

We understand that the ARC is a conglomerate-wide recognition program that aims to better serve the premium clients of the Ayala group – AC Automotive (Ayala-owned Honda, Isuzu, Volkswagen dealerships), Ayala Land Inc., Bank of the Philippine Islands, and Globe Telecom.[1] It is a members-only program which is valid for five years and subject for review and renewal by the ARC management.[2] Members enjoy benefits such as:

[1] ARC, About Ayala Rewards Circle, available at https://www.ayalarewardscircle.com/about/, (last accessed: 10 August 2018).
[2] Id.

- Access to 24/7 domestic and international concierge services;
- Priority handling at BPI branches Preferred lanes and select Globe stores;
- Special deals and discounts from Ayala-owned Honda, Isuzu and Volkswagen dealerships;
- Ayala property promos and exclusive room rates at Ayala Hotels and Resorts;
- Privileges from local and international dining, shopping and leisure partners; and
- Invites to exclusive events both here and abroad.[3]

ARC Terms and Conditions of Membership

Section 3.11 of the 2013 ARC Terms and Conditions provides as follows:

> "3.11 I fully understand and acknowledge that in order for AGCC to provide and maintain the Program and for me to continue enjoying the rewards/benefits of said Program, AGCC will need to collect, process, record, organize, store, update, retrieve, consult, use and/or consolidate all information about me to determine suitable promotions, activities, and products that I can participate in or avail of. For this purpose, I hereby authorize AGCC to obtain updated information about me from the Bank of Philippine Islands (BPI), Globe Telecom, Ayala Land, and other AGCC affiliates, subsidiaries and Partners under an obligation of confidentiality, and to process, use, store, disclose and share such information for the purpose of implementing the Program, as well as for marketing, communication ansd research purposes. I expressly authorize BPI, Globe Telecom, Ayala Land, and other AGCC affiliates, subsidiaries and Partners, to disclose and share, from time to time, to AGCC, any and all information relating to me as appearing in their records, files and databases, including, but not limited to, those relating to my personal information, account information and dealings with them. In this connection, I hereby waive my rights under the confidentiality and data privacy laws of the Philippines and other jurisdictions, and agree to hold BPI, Globe Telecom, Ayala Land and other AGCC affiliates, subsidiaries and Partners, free and harmless from any and all liability that may arise from, or in connection with, the collection, processing, recording, updating, consolidation, disclosure, sharing, use and storage of information relating to me, my accounts and dealings, pursuant to, and in compliance with, the authorization conferred by me under these Terms and Conditions."

[3] Id.

This is followed by the following statements:

—— I have carefully read and understood the foregoing Terms and Conditions and my signature below signifies my express conformity and agreement thereon.

—— I do not accept the foregoing Terms and Conditions and opt not to join the AGCC Program.

_____

Signature above printed name

_____

Date signed

We understand that the above Terms and Conditions was amended in October 2017, and the above provision is now covered under Sections 3.11 and 3.12., to wit:

> "3.11 To maintain and implement the Program in connection with its marketing, communication, analysis and research objectives and for me to continue enjoying the rewards, privileges and benefits thereof, I acknowledge and agree that Ayala Group Club, its directors, officers, employees, service providers, authorized representatives and agents (collectively, the "Ayala Group Club"):
>
> - will collect, obtain, use, store, process and consolidate (collectively, "process" or "processing") information about me (including my Personal Data, contact details, demographic information and account details) to determine suitable promos, events, activities, products and services that I can participate in or avail; and
> - may outsource the processing thereof to service providers, whether within or outside the Philippines, with my consent herein given.
>
> 3.12 By continuing with my ARC membership or by availing of the rewards/privileges/benefits of the Program, I authorize Ayala Group Club, its related companies (including member-companies), assignees and their respective outsourced service providers to use, share and disclose my information for any or all of the following purposes:
>
> - To facilitate the administration, provision, implementation and monitoring of my rewards, benefits and privileges as ARC member;
> - To contact or reach out to me through phone calls, mail,

email, SMS and e-commerce platforms or any other type of electronic facility which the Ayala Group Club may deem appropriate and provide me with marketing or promotional information and materials relating to promos, events, activities, products and services which I may find interesting;

- To develop, enhance and provide improvements/upgrades in its systems and business processes, including but not limited to data analytics and automated processing;
- To carry out and implement the Program promos, events, activities, products and services which I avail of or participate in from time to time.

For any or all of the foregoing purposes, I expressly authorize, from time to time, under an obligation of confidentiality: (i) the Bank of the Philippine Islands, Globe Telecom, Ayala Land, Inc., other Ayala Group Club members, their respective subsidiaries and affiliates (collectively, the "Ayala Group of Companies") and the marketing and promotional partners and third parties, whether within or outside the Philippines (the "Program partners"), to disclose and share to Ayala Group Club my information as appearing in their respective records; and (ii) for the Ayala Group Club to process my updated information obtained from the Ayala Group of Companies and the Program partners. I agree to inform Ayala Group Club of any changes relating to my information through its support@ayalarewardscircle.com.

The foregoing constitutes my express consent under the applicable confidentiality and data privacy laws of the Philippines and other jurisdictions and I agree to hold the Ayala Group Club, the Ayala Group of Companies, the Program partners and their respective authorized representatives and outsourced service providers free and harmless from any and all liabilities, claims, damages, suits of whatever kind and nature, that may arise in connection with the implementation and compliance with the authorization conferred by me under these Terms and Conditions.

I acknowledge that I have received, read, and understood the Program requirements and the foregoing Terms and Conditions and Privacy Policy, and that a representative of Ayala Group Club has fully explained to me the same. By signing below, I am agreeing to the foregoing Terms and Conditions of Membership."[4]

[4] ARC, Terms and Conditions of Membership, available at https://www.ayalarewardscircle.com/terms-and-agreement/ (last accessed: 10 August 2018).

Lawful processing of personal data; consent vis-à-vis fulfillment of a contract as a criteria for lawful processing of personal information

There are several criteria for processing personal and sensitive personal information provided for under Sections 12 and 13 of Republic Act No. 10173,[5] known as the Data Privacy Act of 2012 (DPA).

Processing of personal information may be based on consent, contract, legal obligation, legitimate interest, among others. Similarly for sensitive personal information, the processing thereof may be based on consent, law or regulation, legal claims, among others.

As to the consent of the ARC members to the October 2017 Terms and Conditions, we note that there is a statement in the last paragraph – **"xxx By signing below, I am agreeing to the foregoing Terms and Conditions of Membership."** We assume that these Terms and Conditions were duly sent to all ARC members and in effect, those who signed the document agreed to the new terms and conditions.

Nonetheless, we wish to reiterate the definition of consent as follows:

> "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."

Further, the IRR states that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose.[6] The time-bound element does not necessarily mean that a specific date or period of time has to be declared. Thus, for instance, declaring that processing will be carried out for the duration of a contract between the PIC and the data subject may be a valid stipulation.

Also, as long as the purpose, scope, method and extent of the processing remain to be the same as that disclosed to the data subject when consent was given, the consent remains to be valid.

[5] 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).
[6] Id. § 19 (a) (1).

Hence, considering that only formal changes were made in the 2017 ARC Terms and Conditions, and that no changes were made which affects the purpose, scope, method and extent of the processing of personal data, the consent given under the 2013 ARC Terms and Conditions remains to be valid.

Transparency; rights of the data subjects to be informed and to object

The principle of transparency mandated by the DPA dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[7] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[8]

Thus, in line with the right to information of the data subject, personal information controllers (PICs) are required to apprise the data subject of the following:

1. Description of the personal data to be processed;
2. Purposes for processing, including: direct marketing, profiling, or historical, statistical or scientific purpose;
3. Basis of processing (legal or statutory mandate, contract, etc.)
4. Scope and method of processing;
5. Recipient/classes of recipients to whom the personal data are or may be disclosed;
6. Identity and contact details of the Personal Information Controller;
7. Retention period; and
8. Existence of rights as data subjects.

The above may be operationalized through a privacy notice. A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[9] It is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.[10]

Having stated that, there is also a need to determine and clarify the distinction between privacy policy and securing the consent of the data subject for the processing of his or her personal information.

---

[7] Rules and Regulations implementing RA No. 10173 (IRR), § 18 (a).
[8] Id.
[9] IAPP, Glossary of Privacy Terms, available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2
[10] Id.

Being a mere notice, it is emphasized that the privacy policy or notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects.

Lastly, we note the last paragraph of Section 16(b) of the DPA which states that any information supplied or declaration made to the data subject shall not be amended without prior notification of data subject. This is to be read in connection with the right to object under Section 34(b) of the IRR which in turn states that the data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) LEANDRO ANGELO Y. AGUIRRE
Officer-in-Charge and
Deputy Privacy Commissioner
for Data Processing Systems

ADVISORY OPINION
NO. 2018-59

04 October 2018

[redacted]

Re: SKIP TRACING AND PROBING OF CONTACT DETAILS THROUGH THE INTERNET AND THIRD PARTIES

Dear [redacted],

We write in response to your inquiry about the applicability of the Data Privacy Act of 2012[1] (DPA) to the practice of skip tracing and probing of collection agencies, particularly on the following points:

1. Whether the DPA prohibits collection agencies to obtain and use contact information of a borrower or subscriber made publicly available online, otherwise known as skip tracing; and
2. Whether collection agents are allowed to ask third parties, over the phone or in person, for the updated contact details and address of borrowers in case they can no longer be reached through the contact information you possess, which is known as probing.

The DPA does not prohibit the collection of personal information through skip tracing or probing, provided that the collection or any further processing is done in accordance with the law. In general, processing of personal data should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.[2] There should be procedures in place for data subjects to exercise their rights[3] and appropriate security measures for data protection.

It should be clarified that the public availability of personal information does not exclude it from the scope of the DPA. This law applies to the processing of all types of personal information, publicly available or not,

[1] 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 (15 August 2012).
[2] Data Privacy Act of 2012, § 11-13, 20-21
[3] Data Privacy Act of 2012, § 16.

and to any natural and juridical person involved in personal information processing.[4] "Processing" in this context refers to the collection, use, storage, disposal and any other operation performed upon personal information.[5]

As your inquiry concerns publicly available personal information, it may be useful to note that personal information is considered publicly accessible if:

- The information about an individual is readily observed through reasonably expected means at a public location where the individual appears;
- The information has been manifestly made public by the data subject; or
- The information is obtained from sources that are intended to be accessible to any member of the public.

Collection agencies are considered personal information processors (PIPs) to whom a personal information controller (PIC) has outsourced the processing of personal data of borrowers. This is due to the nature of their business, which, in general, performs the processing of personal data for the benefit of other companies. As PIPs, collection agencies are expected to process personal data only in accordance with their agreement with a PIC.

The processing of personal data should meet one of the conditions for lawful processing provided in Sections 12 and 13 of the DPA, for personal information and sensitive personal information, respectively. One of the conditions that may be applicable in this case is "legitimate interest." The DPA provides that processing of personal information is permissible when it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed.[6]
It should be noted that the processing under this ground shall only involve personal information like contact details and addresses of borrowers. The DPA does not provide legitimate interest as criteria for lawful processing of sensitive personal information.

To determine if there is "legitimate interest" in processing personal information, PICs must consider the following:[7]

[4] Id., § 4.
[5] Id., § 3(j).
[6] Id., § 12(f).
[7] See generally, Data Privacy Act of 2012, § 12(f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on June 11, 2018].

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.

Legitimate interest refers to matters that are desired by or important to a personal information controller (PIC) or third party, which must not be contrary to law, morals or public policy. This includes business, financial, or any other reasonable purpose. The legitimate interest pursued by the PIC or by a third party or parties to whom the data is disclosed should be clearly identified, and the reasonable purpose and intended outcome clarified.[8] The PIC to whom a debt is owed and the third-party agency to whom collection is outsourced may have a legitimate interest to pursue and satisfy the debt.

It is not enough, however, to simply establish the purpose of processing personal information and how it will serve the interests of the PIC for legitimate interest to be considered as lawful basis of processing. The necessity of the particular processing operations should be evaluated. Legitimate interest will not justify intrusive practices, such as harassment, deceptive practices, or vexatious procedures, for these are not necessary to realize the legitimate interests.

Furthermore, while collection agencies may ask third parties such as employers and relatives for updated contact details of borrowers, these third parties are not obligated to give such information, absent a lawful basis for such disclosures. In communicating with third parties, collection agencies should also be mindful of what information to disclose, and whether the same may unduly prejudice the data subject.

PICs have the obligation to balance their legitimate interests against the interests, rights, and freedoms of the data subject considering the particular circumstances relevant to the processing. Legitimate interest

[8] See generally, United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on June 11, 2018].

is not intended to be a broad justification for all purposes assumed by PICs. NPC may evaluate whether legitimate interest is the proper basis for the specific processing, considering the interpretation clause under Section 38 of the DPA, where the law is liberally interpreted in a manner mindful of the rights and interests of the data subject. PICs are advised to determine whether data subjects could be better protected by using other lawful criteria for processing.

The interests and fundamental rights of the data subject could in particular override the interest of the personal information controller where personal data is processed in circumstances where data subjects do not reasonably expect further processing.[9] PICs must also consider the reasonableness of the means employed for processing personal data. In general, personal data should be processed fairly, lawfully, and in a transparent manner.[10] These may include ensuring that only necessary information is collected, using information only to the extent necessary for debt collection, and providing adequate notice to data subjects about how their personal information may be processed.

For instance, where "skip tracing" involves automated processes, the PIC may have separate obligations to provide information on such methods to data subjects, and even to notify the NPC, where such automated processing becomes the sole basis for any decisions that will significantly affect the data subject. Data subjects also have a right to information relevant to the methods of collection and sources of information.

While skip tracing and probing for purposes of pursuing the debt are not prohibited if done in accordance with the provisions of the DPA, the PICs and collection agencies should likewise comply with other applicable laws or regulations on consumer protection and fair collection practices.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [General Data Protection Regulation], Recital 47.
[10] Data Privacy Act of 2012, § 11, 16.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-60

30 August 2018

[redacted]

Re: DISCLOSURE OF PERSONAL INFORMATION TO THE BANGKO SENTRAL NG PILIPINAS

Dear [redacted],

We write in response to your inquiry seeking clarification on Section 4 of Republic Act No. 10173,[1] also known as the Data Privacy Act of 2012 (DPA) in relation to the Bangko Sentral ng Pilipinas' (BSP) examination of financial institutions, pursuant to its supervisory and regulatory powers.

We understand that the Public Safety Savings and Loan Association, Inc. (PSSLAI) is a non-stock, non-profit corporation engaged in the business of accumulating the savings of its members. PSSLAI's membership is limited to the public safety personnel under the Department of Interior and Local Government (DILG), which includes the members of the Philippine National Police (PNP), Bureau of Fire Protection (BFP), and Bureau of Jail Management and Penology (BJMP), among others.

The PSSLAI is a financial institution subject to BSP regulation. Every year, the BSP conducts on-site examination of PSSLAI's books and records, business affairs, administration and financial condition.

We understand, based on your letter, that the BSP requests for information of your members, particularly their personal addresses. You are of the opinion that such disclosure is irrelevant to the BSP's examination and has implications on the safety and security of such members.

[1] 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).

You would like to seek guidance on the extent of the BSP's authority to request for information. Specifically, whether PSSLAI can disclose to the BSP, during its examination, personal information pertaining to your members without the latter's consent.

You likewise ask for clarification on the limitations to BSP's authority and the conditions that must be met for the exercise of the same taking into consideration the provisions of the DPA.

Exclusions from the scope of the DPA

Under Section 4(e) of the DPA, information necessary in order to carry out the functions of public authority is excluded from the scope of the law. This includes the processing of personal data for the performance by the independent central monetary authority its constitutionally and statutorily mandated functions.

The exclusion above is not absolute. The exclusion of the information specified in Section 4 of the DPA is only to the minimum extent necessary to achieve the specific purpose, function or activity. Given this, the personal and sensitive personal information (collectively, personal data) enumerated in Section 4 may be lawfully processed by a personal information controller (PIC), even without meeting the conditions under Sections 12 and 13 of the DPA, but the processing shall be limited to that necessary to achieve the specific purpose, function or activity. The PIC is still required, however, to implement measures to secure and protect the personal data.

We reiterate that the exclusion particularly pertains to information necessary in carrying out the functions of the BSP. This does not mean that all information collected by the BSP is outside the scope of the DPA. Being an exception to the rule, it must be established that the information claimed to be outside the scope of the DPA is:

1. Necessary in order to carry out the functions of the public authority; and
2. Processing of personal data is for the fulfillment of a constitutional or statutory mandate.

Thus, only the information required to be processed pursuant to the said function are not covered by the law, while the BSP, as an entity, is still covered by the DPA. The BSP is mandated under the DPA to adhere to the data privacy principles of transparency, legitimate purpose and proportionality, implement appropriate security measures for personal

data protection, and ensure that data subjects are able to exercise their rights as provided for by law.

Mandate of the BSP; request for personal addresses of PSSLAI's members

Based on a formal communication with the BSP, the "information on the addresses of members is necessary in order to: (i) conduct direct confirmation of loan accounts with the end in view of ascertaining the facts relative to the loans and true condition of PSSLAI; and (ii) determine whether the Association complies with the regulatory requirement, pertinent to the well-defined group statutory provision, to obtain the minimum information, such as addresses, of its members."

Further, the BSP stated that the director and examiners of the concerned department is authorized to compel the presentation of all books, documents, papers or records necessary in their judgement to ascertain the facts relative to the overall condition of any Association or to any loan, pursuant to Section 22 of Republic Act No. 8367 or the Revised Non-Stock Savings
and Loan Association Act of 1997.

In this case, the BSP, having a constitutional[2] and statutory[3] mandate to collect and process personal data, may do so even without the consent of the data subjects. But this is with the concomitant responsibility of ensuring that organizational, physical, and technical security measures are in place to protect the personal data it is processing.

In addition, we trust that the BSP is well aware of its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, which requires all government agencies engaged in the processing of personal data to observe the following duties and responsibilities:

A. through its head of agency, designate a Data Protection Officer;
B. conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data;
C. create privacy and data protection policies, taking into account the privacy impact assessments;
D. conduct a mandatory, agency-wide training on privacy and data

[2] 1987 Phil. Const. Art. XII, § 20.
[3] An Act Providing For The Regulation Of The Organization And Operations Of Banks, Quasi-Banks, Trust Entities And For Other Purposes [THE GENERAL BANKING LAW OF 2000], Republic Act No. 8791 (2000), § 4; THE NEW CENTRAL BANK ACT, Republic Act No. 7653 (1993), § 25 and 28

protection policies once a year, and that a similar training shall be provided during all agency personnel orientations;

E. register its data processing systems with the NPC;

F. cooperate with the NPC when the agency's privacy and data protection policies are subjected to review and assessment.

Should you wish to seek additional guidance and clarification, you may communicate with the BSP's Data Protection Officer at this email address: dataprotection@bsp.gov.ph.

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-61

06 September 2018

[redacted]

Re: PROCESSING OF PERSONAL INFORMATION FOR CHARACTER REFERENCE

Dear [redacted],

We write in response to your request for an advisory opinion regarding the applicability of Section 12(f) of the Data Privacy Act of 2012 (DPA)[1] as a basis for the processing of the name and contact number of character references that were supplied by an applicant for a loan, making the processing permissible even without the consent of the said character reference.

We understand that HC Consumer Finance Philippines, Inc. (Home Credit) is a financing company whose primary purpose is to extend loans, credits and all types of financial accommodations from its own capital without collateral. To support the loan collection process, the company requires applicants and borrowers to supply at least two (2) character references and their respective contact numbers.

The name and contact information of the character reference are considered personal information, and the processing of such information shall be permitted only if not otherwise prohibited by law, and when at least one of the conditions set by the Section 12 of the DPA is met.

Among the criteria provided in the law for the processing of personal information is when "the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by

[1] 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).

a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."[2]

Legitimate interest refers to matters that are desired by or important to a personal information controller (PIC), which must not be contrary to law, morals or public policy.[3] This includes business, financial or other reasonable purpose. The legitimate interest pursued by the PIC or by a third party or parties to whom the data is disclosed should be clearly identified, and the reasonable purpose and intended outcome clarified.[4] In order to use legitimate interest as criteria for lawful processing, PICs must consider the following:[5]

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test- The fundamental rights and freedoms of data subjects should not be overridden by the legitimate interests of the PICs, considering the likely impact of the processing on the data subjects.

We also note Recital 47 of the General Data Protection Regulation (GDPR) which states that the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.[6]

Taking into account that the sole purpose of Home Credit in requesting the names and contact numbers of the character references is to ask for additional information about the applicant or borrower, such as new address and/or new contact number of the applicant or borrower, in the event that the latter defaults in his/her loan obligation and can no longer

[2] Id, §12(f).

[3] See also United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018] (Anything illegitimate, unethical or unlawful is not a legitimate interest).

[4] See generally, United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018].

[5] See generally, Data Privacy Act of 2012, § 12(f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018].

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119), Recital 47.

be reached at the contact information he/she provided, the same may be considered as a legitimate interest of Home Credit for verification and fraud prevention.

The NPC may evaluate whether the PIC correctly relied on legitimate interest as the proper basis for the specific processing, taking into consideration the interpretation clause of the DPA under Section 38, and whether the rights of the data subject could be better protected by using the other lawful criteria for processing.

However, taking into consideration the rights of data subjects, it is likewise advisable that moving forward, Home Credit should endeavor to make changes in the processing of loan applications and the forms necessary for the same, i.e. the loan application or contract with the borrower may reflect that the borrower guarantees and certifies that the character references have been informed by the borrower that his or her personal details will be submitted to Home Credit and that he or she consented to the processing of their personal information. It is important to specify that personal information will only be used to achieve the above-mentioned purposes.

As it is the applicants or borrowers that supply the character references to Home Credit, it is incumbent upon them to seek the approval of these references that they have selected if they indeed consent to the use of their personal information.

Further, there should be a manual of operations on how Home Credit and its employees or agents handle calls with character references should Home Credit proceed to contact these persons.

For instance, it is advisable that at the start of the call, the data subject be adequately informed of the purpose of the same, how Home Credit obtained his or her contact details, ask for consent to continue with the call, provide the option of ending the call should the data subject wish to do so, clarify that they may be contacted again in the future should it be necessary, provide the option also of having their personal data removed as a character reference, if the same is feasible, etc.

All of these should take into account the data privacy principles of transparency, legitimate purpose and proportionality, and upholding the rights of data subjects.

Finally, we emphasize that the NPC may prescribe or determine, in certain cases, the proper criteria for lawful processing of personal data.

It can also determine whether there is a violation of the provisions of the DPA, and consequently, recommend to the Department of Justice the prosecution of crimes and imposition of penalties specified in the law.

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.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-62

11 September 2018

[redacted]

Re: DISCLOSURE OF PERSONAL DATA OF PATENT AND TRADEMARK APPLICANTS AND INVENTORS

Dear [redacted],

We write in response to your request for an advisory opinion seeking clarification on the sharing of personal data of patent and trademark applicants and inventors by the Intellectual Property Office (IPOPHL) to the World Intellectual Property Office (WIPO) and the First IP Consultancy and Technical Services Co. (First IP) vis-à-vis the provisions of the Data Privacy Act of 2012[1] (DPA) and its Implementing Rules and Regulations[2] (IRR). You also inquired if a data sharing agreement is needed should disclosure be allowed.

We understand that the WIPO is an international organization created to promote worldwide protection of intellectual property creations. It is requesting for personal data of patent and trademark applicants and inventors registered with the IPOPHL, in particular, their names, addresses, e-mail addresses, telephone numbers, and nationalities. The requested data shall be used for the Committee in Development and Intellectual Property (CDIP) project on the ASEAN Design Study. Specifically, the requested data is needed to understand the role of industrial designs in business strategies being done by high, low, and middle income countries.

We understand further that First IP, a private firm, is also requesting the list of inventors and applicants and their contact details from the Visayas region. The purpose is to identify the inventors in the region in order to

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

organize them under the Visayas Chapter of the Filipino Inventor Society.

Publicly available data; pending patent and trademark applications

Based on your separate email clarification, you made a distinction between published or registered applications for patent and trademarks, and those which are still pending evaluation.

We understand that all patent and trademark applications that are already published or registered are publicly available information, and the same may be viewed in your website and library. With this, personal data of registered and published applicants and inventors may be disclosed to WIPO as these are already publicly available information and WIPO's processing is for research.

Note that personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards is excluded from the scope of the DPA, to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned.[3]

Considering the principle of proportionality, where the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, IPOPHL may share the information limited to that which is necessary to the research purpose of WIPO.

It is likewise advisable for IPOPHL to include an appropriate statement on its privacy notice regarding the data to be shared with the WIPO. The principle of transparency dictates that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[4] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[5]

As to First IP's request, you may direct them to the appropriate website and/or repository of the personal data that they require which is available to the public in general. As their processing is for the purpose of soliciting new members for their organization, they would have the responsibility

[3] Id., §5(c)
[4] Id., §18(a).
[5] Id.

of obtaining the consent of these inventors and applicants should First IP proceed to contact them individually.

For the pending patent and trademark applications, we understand that these are kept confidential pursuant to internal policies. You confirmed that the information and other matters related to pending applications are held in utmost secrecy, until such time that they are published or registered in accordance with the novelty requirement under the Intellectual Property Code.

Thus, the disclosure of the personal data relating to pending patent and trademark applicants and inventors to the WIPO and to First IP may only be allowed if said applicants and inventors have given their consent, specific to the respective declared purpose of the data sharing.[6]

Data sharing

Under the IRR, data sharing is defined as the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal processor.[7] In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned.[8]

Data sharing may be allowed under any of the conditions set forth in the DPA and its IRR, as when it is expressly authorized by law provided that there are adequate safeguards for data privacy and security, and the data privacy principles of transparency, legitimate purpose are adhered to.[9] Furthermore, data sharing may be allowed in the private sector if the consent of the data subject is obtained, and the specific conditions under the IRR are met.[10]

Note also that data collected from parties other than the data subject for the purpose of research may be allowed when the personal data is publicly available, or has the consent of the data subject, as long as adequate safeguards are in place and no decision directly affecting the data subject will be made on the basis of the data collected or processed.[11]

Hence, the execution of separate data sharing agreements with both WIPO and First IP, respectively, is highly recommended for the sharing of personal data relating to the pending patent and trademark applicants

[6] Data Privacy Act of 2012, §12 (a) and §13 (a).
[7] Id. § 3 (f).
[8] Id.
[9] Rules and Regulations Implementing the Data Privacy Act of 2012, § 20 (a).
[10] Id. § 20 (b).
[11] Id., § 20 (c).

and inventors to ensure that there are adequate safeguards for data privacy and security implemented by both parties. For proper guidance, please refer to NPC Circular No. 2016-02 – Data Sharing Agreements Involving Government Agencies.

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.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-63

23 October 2018

[redacted]

Re: REVIEW OF CONSENT FORM

Dear [redacted],

We write in response to your request to review the Armed Forces and Police Savings and Loan Association, Inc. (AFPSLAI) Data Privacy Consent Form template.

We wish to emphasize that there is no requirement under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and issuances of the NPC to have the various consent forms reviewed and approved by the NPC. Nonetheless, we take this opportunity to elucidate the concept of consent under the DPA and how this may be operationalized.

Section 3(b) of the DPA defines consent of the data subject as 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.

The EU General Data Protection Regulation (GDPR) offers further interpretation on consent:

> "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could

include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."[1]

Based on the discussions above, it is evident that the consent contemplated by the law is an express consent wherein the data subject voluntarily assents to the collection and processing of personal information, rather than an implied or inferred consent.

Likewise, consent should be specific. The limitation emphasizes that consent cannot be overly broad for this would undermine the very concept of consent. For instance, a "bundled"consent will generally not suffice as the data subject is not empowered to make a true choice.

The following are our observations for your consideration:

Purposes of processing personal data

AFPSLAI requires the consent of the members for the following:

a. AFPSLAI operations [e.g. membership profile, accounts management, loans management, billing & collection, and other business operations];
b. research and business development or other initiatives to further improve or update product lines or service delivery;
c. for promotions or marketing initiatives through mail, email, fax, SMS, telephone, or any other means of communication;
d. collection of loans and receivables, past due and written-off accounts; and
e. payment of loan proceeds and other disbursements.

All of the above are enumerated and combined in a single paragraph. As mentioned, consent, where required, should be specific. Having an

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119), Recital 32.

enumeration of each and every purpose of the processing in a single paragraph, while providing for specificity, still fails to provide the data subject with a genuine choice as he or she will still be bound to sign off on the entire provision in toto.

Note also that the basis of the lawful processing of some of the above items is not consent. Rather, it may be processing of personal information that is necessary and is related to the fulfillment of a contract or in order to take steps at the request of the data subject prior to entering into a contract,[2] or may be necessary for compliance with a legal obligation,[3] or necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed.[4]

For sensitive personal information, the processing is provided for by existing laws and regulations,[5] or necessary to achieve the lawful and noncommercial objectives of public organizations and their associations[6] (for non-stock savings and loan associations), or necessary for the establishment, exercise or defense of legal claims.[7]

Hence, a separate consent need not be obtained for purposes which do not require consent of the members.

We note that there is also a statement in the form that the consent shall automatically expire ten (10) years from the last transaction. There may be a need to clarify what will happen to the personal information after the expiration of the consent, i.e. will this serve as a retention period as well, in addition to the disposal of records based on existing laws and internal policy?

We emphasize that where applicable, such as in cases where the period of processing can be reasonably ascertained at the time of collection, a PIC may specifically provide for the period of validity of a consent obtained from a data subject. It is worth noting that the limitation merely emphasizes that consent cannot be overly broad and perpetual, for this would undermine the very concept of consent, as defined in the law.

Personal data collected

The listing of personal data (personal information and sensitive personal information) being processed was also provided in the form, but it is

[2] Data Privacy Act of 2012, § 12 (b)
[3] Id., § 12(c)
[4] Id., § 12(f)
[5] Id., § 13(b)
[6] Id., § 13(d)
[7] Id., § 13(f)

necessary to determine which personal data is processed for what particular purpose, following the general data privacy principles of transparency, legitimate purpose and proportionality.

For instance, the information on beneficiary/ies such as name, age, birthdates, addresses, and sources of funds may not be necessary and proportional for the processing in relation to promotions or marketing initiatives of AFPSLAI.

Also, considering the proportionality principle and practicing data minimization, there is a need to re-evaluate if indeed, all of the listed personal data is absolutely necessary for AFPSLAI's processing activities. We reiterate that personal information must be adequate and not excessive in relation to the purposes for which they are collected and processed.[8]

In order to make this determination, the conduct of a privacy impact assessment (PIA) is necessary. Please refer to NPC Advisory No. 2017-03 on Guidelines for Privacy Impact Assessments for further information. This is available at our website at https://privacy.gov.ph/wpcontent/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf.

Privacy Notice

The provisions of the draft form may actually form part of the privacy notice of AFPSLAI. A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[9] A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.

This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects. Being a mere notice, it is emphasized that the privacy notice is not equivalent to consent. Obtaining consent from the data subject for the purposes of processing his or her personal data is a different requirement altogether.

The NPC observed that the Data Privacy Protection Notice in the website is not prominently placed as one may find it under the About Us – Announcements tab, lumped with other AFPSLAI announcements (http://www.afpslai.com.ph/info_ announcements.php), making it difficult for data subjects to view the same. Taking into consideration

[8] Id., § 11(d)
[9] IAPP, Glossary of Privacy Terms, available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2

the transparency principle, there is a need to re-evaluate the placement of the notice in the website and make sure that link to the same is visible and accessible.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) LEANDRO ANGELO Y. AGUIRRE
Officer-in-Charge and
Deputy Privacy Commissioner
for Data Processing Systems

ADVISORY OPINION
NO. 2018-64

11 September 2018

[redacted]

Re: CLARIFICATIONS ON ISSUANCE OF PRESS RELEASES BY THE PHILIPPINE DEPOSIT INSURANCE CORPORATION

Dear [redacted],

We write in response to your request for an advisory opinion regarding the non-applicability of the Data Privacy Act of 2012 (DPA)[1] and its Implementing Rules and Regulations (IRR) on the press releases which the Philippine Deposit Insurance Corporation (PDIC) issues in its capacity as insurer of bank deposits, risk mitigator, together with other financial regulators, and as the statutory liquidator of closed banks based on Section 4(e) of the DPA.

Section 4 of the DPA states that the law is applicable to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Likewise, it provides for certain personal information excluded from its scope – one of which is personal information necessary in order to carry out the functions of public authority, including the processing of personal data for the performance by the regulatory agencies of their constitutionally and statutorily mandated functions.[2]

Note that the exclusion above is not absolute. The exclusion of the information specified in Section 4 of the DPA is only to the minimum extent necessary to achieve the specific purpose, function or activity.

[1] 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).
[2] Id., § 4(e).

Given this, the personal and sensitive personal information enumerated in Section 4 may be lawfully processed by a personal information controller, even without meeting the conditions under Sections 12 and 13 of the DPA, but the processing shall be limited to that necessary to achieve the specific purpose, function, or activity. The PIC is still required, however, to implement measures to secure and protect personal information.

We understand that the PDIC is mandated to promote and safeguard the interests of the depositing public[3] and to generate, preserve, maintain faith and confidence in the country's banking system, and protect it from illegal schemes and machinations.[4]

To do this, we understand that PDIC issues and posts press releases pertaining to cases filed by the PDIC against former bank officers, shareholders, and employees of closed banks for unfair and unsound banking practices under the PDIC Charter, and for fraud, irregularities, and anomalies discovered as a result of investigations conducted by the PDIC.

The DPA, on the other hand, has the twin task of protecting the fundamental human right of privacy and ensuring the free flow of information to promote innovation and growth. The law will not operate to hinder the PDIC from publishing certain items of personal information it deems crucial that the public be informed of, anchored on its mandate discussed above.

We refer you to Advisory Opinion No. 2017-035 dated 27 July 2017, addressed to [redacted] of the PDIC where the same issue was briefly discussed, to wit:

> "If it is within the mandate of the PDIC to publish reports on cases or complaints filed by the PDIC in order to inform the public, the DPA will not operate to hinder the said mandate.
>
> We note however that there may be a need to check other pertinent laws, jurisprudence, rules and regulations which provide for the confidentiality of records of court proceedings or information from proceedings."

Furthermore, said publication should also adhere to the principle of proportionality especially since it would involve public disclosure of personal information. The principle requires that "the processing of

[3] An Act Establishing the Philippine Deposit Insurance Corporation, Defining its Powers and Duties and for other Purposes [PDIC CHARTER] Republic Act No. 3591 (1963), as amended, § 1.
[4] Id., § 2.

information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if purpose of the processing could not reasonably be fulfilled by other means.[5]

This opinion is being rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[5] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(c) (2016).

ADVISORY OPINION
NO. 2018-66

08 November 2018

[redacted]

Re: SUBMISSION OF REQUIRED PERSONAL DATA OF PATIENTS WHO UNDERGO DRUG TESTING TO THE DEPARTMENT OF HEALTH

Dear [redacted],

We write in response to your inquiry regarding the submission drug test results and other personal data of patients by Grepa Medical and Diagnostic Center (GMDC) to the Department of Health (DOH) through the Integrated Drug Testing Management Information System (IDTOMIS).

Particularly, your main concern is whether the submission of the required personal data of patients who undergo drug testing is consistent with the general data privacy principles enshrined in the Data Privacy Act of 2012 (DPA)[1] given the following situations:

In terms of transparency and legitimate purpose, the DOH may share the personal data of patients who undergo drug testing with other government agencies; and in terms of proportionality, the DOH collects personal data of other persons, i.e. name of the spouse of the person being tested.

We understand that as an accredited drug testing laboratory, GMDC is required to use IDTOMIS to submit to the DOH all required personal data of patients who undergo drug testing.

Also, that the IDTOMIS is a system implemented by the DOH to facilitate collection of data for accrediting drug testing laboratories and

[1] 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).

rehabilitation centers, drug testing operations as compliance to the mandate given to the DOH by Republic Act No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002.[2]

Legitimate purpose

Under the DPA and its Implementing Rules and Regulations (IRR), the principle of legitimate purpose pertains to the processing of personal information based on the declared and specified purpose, which is not contrary to law, morals or public policy.[3] Lawful processing, on the other hand, is discussed under Sections 12 and 13 of the DPA for processing of personal information and sensitive personal information, respectively.

In consideration of the foregoing, we confirm that the submission of personal data of patients who undergo drug testing by GMDC to the DOH, through the IDTOMIS, as well as sharing of the such information by the DOH to authorized government agencies, is permitted[4] pursuant to the provisions of the Comprehensive Dangerous Drugs Act of 2002, to wit;

> "Section 76. The Duties and Responsibilities of the Department of health (DOH) Under this Act. – The DOH shall:
>
> (1) Oversee the monitor the integration, coordination and supervision of all drug rehabilitation, intervention, after-care and follow-up programs, projects and activities as well as the establishment, operations, maintenance and management of privately-owned drug treatment rehabilitation centers and drug testing networks and laboratories throughout the country in coordination with the DSWD and other agencies;"[5]

The lawfulness of the processing of personal data through the IDTOMIS is further supported by the DOH Administrative Order No. 2008-0025[6] and the Dangerous Drug Board Regulation No. 8, S. 2007 which states that:

---

[2] An Act Instituting the Comprehensive Dangerous Drugs Act of 2002, Repealing Republic Act No. 6425, otherwise known as the Dangerous Drugs Act of 1972, As Amended, Providing Funds Therefor, and for other purposes [The Comprehensive Dangerous Drugs Act of 2002] Republic Act No. 9165 (2002).

[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (b) (2016).

[4] Id., § 13.

[5] Supra note 2, § 76.

[6] Department of Health, Administrative Order 2008-0025, Guidelines on the Implementation of the Integrated Drug Test Operations and Management Information System (IDTOMIS) for Screening and Confirmatory Drug Test Laboratory Operation (29 July 2008).

> "Section 3. Section 6, Sub-Paragraph 5.2 (Information Technology Requirements) of DDB Regulation No. 2, Series of 2003, is hereby amended, such that the provision shall now read as follows:
>
> xxx
>
> "5.2 The laboratory shall have access to and utilize the Integrated Drug Testing Operations Management Information System (IDTOMIS), which is the Application Service Provider (ASP) approved and maintained by the DOH."" [7]

Notwithstanding lawful processing of personal data, GDMC as personal information controller (PIC) is required to comply with the DPA, its IRR and other relevant issuances, including the implementation of organization, physical and technical security measures, and formulation of data breach protocols. It must be able to safely and securely transfer information to the DOH through the IDTOMIS.

Transparency

The principle of transparency, as discussed by the law and the IRR, pertains to the data subject's awareness of the nature, purpose, the extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the PIC, his or her rights as a data subject, and how these can be exercised.[8]

GDMC, as a PIC, is then required to inform the patients who undergo drug testing regarding the recipients of his or her personal data or the entities to whom personal data are or may be disclosed, including DOH and other authorized government agencies.

The GDMC may exercise the principle of transparency through a privacy notice. A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.[9] A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes, a privacy policy.[10]

---

[7] Dangerous Drugs Board, Board Regulation No. 8 Series of 2007, AMENDING BOARD REGULATION NO. 2, SERIES OF 2003, ENTITLED "IMPLEMENTING RULES AND REGULATIONS GOVERNING ACCREDITATION OF DRUG TESTING LABORATORIES IN THE PHILIPPINES" (11 December 2007).

[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (a) (2016).

[9] IAPP, Glossary of Privacy Terms, "Privacy Notice" available at https://iapp.org/resources/glossary/#paperwork-reduction-act-2 (last accessed on 10 September 2018).

[10] Implementing Rules

Proportionality

In compliance with the principle of proportionality, the DOH and other government agencies, as PICs, should be able to determine and justify the adequacy, relevance, appropriateness of the personal data being collected though IDTOMIS.[11]

With this, we recommend that the GDMC to seek clarification and justification from the DOH regarding the collection of other personal data, specifically the name of spouse of patients who undergo drug testing.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[11] Id, § 18(c) (2016).

ADVISORY OPINION
NO. 2018-67

24 September 2018

[redacted]

Re: OWWA E-CARD PROJECT

Dear [redacted],

We write in response to your request for an advisory opinion which sought to confirm whether the OWWA E-Card Project is a special case within the purview of Section 4(e) of the Data Privacy Act of 2012 (DPA).[1]

As mentioned in your letter, Section 11 of the Overseas Workers Welfare Administration Act (OWWA Act)[2] mandates the OWWA board to issue an OWWA E-Card, identification card or any other proof of membership upon payment of the member's contribution. It likewise directed the OWWA to maintain a comprehensive and updated database of member-Overseas Filipino Workers (OFWs).

Special case under the law

Section 4 of the DPA states that the law does not apply to:

> "e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic

[1] 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" (15 August 2012).
[2] An Act Governing the Operations and Administration of the Overseas Workers Welfare Administration, "Overseas Workers Welfare Administration Act" (10 May 2016).

> Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act NO. 6427, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);"

Based on the provision above, the exemption on information necessary in order to carry out the functions of a public authority shall apply only to the independent central monetary authority, law enforcement, and regulatory agencies. It is then important to evaluate whether OWWA is law enforcement or regulatory agency.

The OWWA is a chartered institution, attached to the Department of Labor and Employment (DOLE) with the function of developing and implementing welfare programs and services for its member-OFWs and their families, and administer the OWWA Fund.[3] It functions as an administrative agency, not as a regulatory or law enforcement agency.

Hence, the processing[4] of personal information for the OWWA e-card project is not exempt from the scope of the DPA.

Lawful processing of personal data

The letter that you have provided us failed to indicate the personal data that will be processed pursuant to the OWWA E-Card Project. However, considering that the stakeholders and data subjects involved are OFWs, it can be derived that sensitive personal information[5] are involved, such as passport details and other government issued identification numbers and details.

Section 13(b) of the DPA states that processing of sensitive personal information is permitted when the processing of the same is provided for by existing law and regulations. The OWWA Act clearly instructed the OWWA to issue any proof of membership upon payment of the required contribution to facilitate in availment of services, participation in welfare programs and receive assistance from the agency.

With this, there is evidently legal and lawful basis for the processing activities by OWWA.

Nevertheless, OWWA as a personal information controller (PIC)[6] shall ensure that processing of personal data of OFWs is in accordance with

[3] Id, §4.
[4] Data Privacy Act of 2012, §3(j).
[5] Id, §3(l).
[6] Id, §3(h).

the general privacy principles of transparency, legitimate purpose and proportionality.[7]

The principle of transparency entails the awareness of the data subjects of the nature, purpose, and extent of the processing of his or her personal information.[8] OWWA must inform the data subjects, the OWWA members in this case, regarding the risks and safeguards involved in the processing, as well as their rights a data subjects, and how they can exercise those rights.

Also, it is important to state that the purpose of processing their personal information is for the E-Card Project, the database and other related programs of the agency.[9] Lastly, OWWA shall ensure that the information collected, used, and stored are all necessary, relevant and not excessive in relation to the declared purpose of processing.[10]

Furthermore, OWWA, as a PIC is duty-bound to comply with the DPA, its IRR and other relevant issuances, including the appointment or designation of a Data Protection Officer, registration of data processing system/s, implementation of organizational, physical and technical security measures, and formulation of data breach protocols, among others.

The diagram of the process flow on the collection, use, processing and issuance of the OFW E-Card illustrates the intervention of a third party for the card printing. Each PIC shall be responsible for personal information transferred to a third-party for processing and shall ensure that agreements and contracts with such third parties have sufficient and appropriate safeguards in place.[11]

This opinion is based solely on the questions propounded and the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. Note that the attached OWWA Privacy Policy was not reviewed for purposes of this advisory opinion.

[7] Implementing Rules and Regulations of the DPA, §11.
[8] Id, §18(a).
[9] Id, §18(b).
[10] Id, §18(c).
[11] Id, §43.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-69

02 October 2018

[redacted]

Re: PHONE USAGE DATA RECORDS

Dear [redacted],

We write in response to your request for an advisory opinion concerning the applicability of the Data Privacy Act of 2012[1] (DPA) to anonymous information.

The DPA does not cover anonymous information. The DPA applies to any processing of all types of personal information, which is 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.[2]

However, the data you request must be truly anonymous, else the provisions of the DPA shall apply.

As recognized by the EU General Data Protection Regulation (GDPR), upon which the DPA is based on, "the principles of data protection should therefore not apply to anonymous information."[3] Information is anonymous when it "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[4] Further, the GDPR

[1] 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).
[2] Data Privacy Act of 2012, § 3 (g).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 26.
[4] Ibid.

does not apply to the "processing of anonymous information, including for statistical or research purposes."[5]

We understand that the CHED-PCARI-DARE project seeks to develop an advanced travel demand prediction and optimization platform that shall be an essential decision support tool for government and transportation professionals.

To this end, Mapúa requested the following information from TelCos:

1. Timestamp;
2. Anonymized User ID;
3. Antenna ID;
4. Base Station Location; and
5. Phone Record Type.

Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party of the European Commission provides an illustration on how a dataset would qualify as anonymous:

> "If an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data."[6]

In view of the foregoing, there is a need to make a determination if, indeed, the enumerated Phone Usage Data Record being requested by Mapúa is anonymous information. If otherwise, the information requested by Mapúa is considered as personal information and its processing is subject to the requirements under the DPA, its IRR and issuances of the NPC.

For your information, the DPA applies to any processing of all types of personal information, which is refers to any information whether recorded in a material form or not, from which the identity of an individual

[5] Ibid.
[6] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, §2.2.2 – Potential identifiability of anonymized data

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.[7]

Under the DPA, the processing of personal data is allowed, subject to its compliance with the statute and other applicable laws. Adherence to the principles of transparency, legitimate purpose, and proportionality is also paramount.

Sections 12 and 13 of the DPA lay down the criteria for the lawful processing of personal and sensitive personal information, respectively. Any permissible processing must rely on at least one of the conditions set out in the law, depending on the type of information involved.

As personal information controllers, Mapúa and Globe are reminded of their obligations under the DPA, which includes the requirement to implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful processing.

Finally, the parties involved in the project must determine conclusively that no personal data will be shared, disclosed, or transferred by the TelCos and/or any other entity to Mapúa. A contrary finding would necessitate the execution of a data sharing agreement (DSA). If a government agency will be party to the DSA, i.e. CHED and/or UP Diliman as mentioned in your letter, the DSA to be executed should be in accordance with the IRR and NPC Circular No. 16-02 - Data Sharing Agreements Involving Government Agencies.

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.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office\

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[7] Data Privacy Act of 2012, § 3 (g).

ADVISORY OPINION
NO. 2018-70

05 October 2018

[redacted]

Re: MUNTINLUPA CITY ORDINANCE NO. 96-80

Dear [redacted],

We write in response to your inquiry which sought to clarify whether City Ordinance No. 96-80, requiring the submission of personal information of the rank and file employees to the Public Employment Service Office (PESO), is permissible under the Data Privacy Act of 2012 (DPA).[1]

City Ordinance No. 96-80[2] directs employers to require submission of the voter's ID or Income Tax Return for pre-employment screening in order to determine the residency of the potential applicant.[3] Furthermore, the PESO is authorized by the city government to require the submission of the following requirements for renewal of business license:

a) List of rank and file employees comprising the seventy percent (70%) who are residents of Muntinlupa;
b) Nature of business;
c) Personal information of rank and file residents:
    1. Age;
    2. Address;
    3. Years of service in the company; and
    4. Current position and job description.[4]

[1] 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).
[2] Kautusang Panlungsod na Nag-Aatas sa lahat ng Kompanya/Bahay-Kalakal na Nagnenegosyo sa Lungsod ng Muntinlupa, na sa pagtanggap ng karaniwang kawani (rank and file), ang hindi bababa sa pitumpung porsiyento (70%) ng manggagawa ay dapat residente ng lungsod (01 July 1996).
[3] Id. § 4.
[4] Id. § 7.

The provisions above make it clear that the ordinance requires the processing of both personal information and sensitive personal information (age) of employees. Thus, the submission of these personal data constitutes a legal obligation on the part of personal information controller.[5]

The legal obligation of employers comes from City Ordinance No. 96-80, which is an ordinance be duly enacted by the city government of Muntinlupa. Cities and municipalities, through their respective **Sangguniang Panlungsod** and **Sangguniang Bayan**, are granted police power to make statutes and ordinances that promote the health, morals, peace, education, good order or safety and general welfare of its constituents.[6] Giving priority to its residents for employment opportunities within the city is part of the functions of the city government based on Section 16 of the Local Government Code, which states that every local government unit (LGU) is mandated to ensure employment and enhance the economic condition of its jurisdiction.

The processing of sensitive personal information is also supported by the DPA, as City Ordinance No. 96-80 satisfies the requirement of an existing law or regulation which requires the processing of sensitive personal information.[7]

The existence of a lawful basis for processing does not give unrestricted authority to any entity to process personal information. Whenever government collects and further processes personal data, the agency must comply with the obligations under the DPA. The processing of personal information requires adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality.

The principle of transparency states that the data subject must be aware of the nature, purpose and extent of processing of his or her personal data. Therefore, the employers, as well as the city government, must inform the employees in clear and plain language that their personal data is required by the LGU for monitoring and legislative purposes.

Second, the processing of personal information shall be compatible with a declared and specified purpose, which is not contrary to law, morals, or public policy. It is a settled rule that an ordinance duly passed by such **Sanggunian** is presumed valid unless and until the courts declare the contrary in clear and unequivocal terms.[8]

---

[5] Id. § 12 (c).
[6] Social Justice Society v. Hon. Jose L. Atienza, G.R No. 156052 (S.C., February 13, 2008) (Phil.), available at http://sc.judiciary.gov.ph/jurisprudence/2008/feb2008/156052.htm
[7] Id. § 13 (b).
[8] Supra note 6.

Lastly, the principle of proportionality states that only adequate, relevant, suitable and necessary information will be processed. The LGU shall require only as much personal data as is needed to directly fulfill the objectives of the regulation. We therefore recommend that the LGU review the requirement for the sensitive personal information of employees, as well as any personal information beyond name and address, to establish if they are necessary to achieve the objective of the ordinance.

The LGU should be able to demonstrate its accountability for the personal data it is collecting under its ordinance, to the end that the data subjects are protected from harm and other privacy risks. Thus, the LGU is also mandated under the DPA to uphold the rights of data subjects. The collection and further processing of these information collected from employers should be safeguarded against illegal or unauthorized processing. Security measures for data protection should be implemented to ensure that the confidentiality, integrity and availability of the personal data are maintained.

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-71

05 October 2018

[redacted]

Re: DISCLOSURE OF SCHOOL RECORDS FOR INVESTIGATION PURPOSES

Dear [redacted],

We write in response to your letter which sought clarification on whether the disclosure of school records for investigation purposes of the National Bureau of Investigation (NBI) is in accordance with Data Privacy Act of 2012 (DPA),[1] its Implementing Rules and Regulations (IRR) and relevant issuances of the National Privacy Commission (NPC).

School records as sensitive personal information

The Education Act of 1982 (Batas Pambansa Blg. 232)[2] promotes and safeguards the welfare and interest of students by defining their rights and obligations. As mentioned in your letter, the law recognizes that schools have the obligation to maintain and preserve the confidentiality of school records.[3] Thus, students, in general, have a reasonable expectation of privacy with regard to their school records.

Personal information about an individual's education and those that are established by law as classified are considered sensitive personal information.[4] The DPA prohibits the processing of sensitive personal information, except in the following cases:

a. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged

[1] 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).
[2] An Act Providing for the Establishment and Maintenance of an Integrated System of Education [Education Act of 1982], Batas Pambansa Blg. 232 (11 September 1982).
[3] Id. § 9 (4).
[4] Data Privacy Act of 2012, § 3 (l).

information, all parties to the exchange have given their consent prior to processing;

b. The processing of the same is provided for by existing laws and regulations: **Provided**, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: **Provided, further**, that the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: **Provided**, that such process is confined and related to the bona fide members of these organizations or their associations: Provided, further, that the sensitive personal information are not transferred to third parties: **Provided, finally,** that consent of the data subject was obtained prior to processing;
e. The processing is necessary for purposes of medical treatment is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
f. The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

Disclosure of school records may not be warranted in this case due to the absence of any of the circumstances which will serve as a lawful basis for the processing of sensitive personal information. The letter-request of NBI does not establish the criteria it relies upon to sufficiently justify why the school should not maintain the confidentiality of the school records.

Processing of personal information by law enforcement agencies

Section 5 of the IRR provides that the DPA does not apply to certain categories of personal information, including those that are necessary to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function. This exemption, however, is only

to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.

For the exclusion to apply, the personal information processed by public authorities must be necessary to carry out their function as a law enforcement agency or regulatory body, and that such processing is in accordance with their constitutional or statutory mandate.

The NBI is created, reorganized, and modernized to enhance the investigative and detective work that it handles.[5] It has express power to request the assistance of law enforcement agencies such as the Philippine National Police (PNP), Armed Forces of the Philippines (AFP) or any other agency of the government in its anti-crime drive.

Thus, it is fundamentally an investigative agency rather than a law enforcement agency. Nevertheless, the NBI is considered a law enforcement agency when statute declares it to be so, such as in the Anti-Child Pornography Act of 2009[6] and the Comprehensive Dangerous Drugs Act of 2002,[7] among others. The letter of the NBI failed to disclose the subject matter of investigation, and it cannot be determined whether it is acting as an investigative agency or as a law enforcement agency and accordingly, exercising its function pursuant to its statutory mandate.

Constitutional guarantee against unreasonable search and seizure

Even if the NBI is acting as a law enforcement agency, the exemptions provided in Section 4 of the DPA (Section 5 of the IRR) apply only to the extent necessary to fulfill its statutory functions, based on the presumed public interest in the processing of these categories of information.

The phrase, "necessary for law enforcement purposes" is not a weapon that can be indiscriminately wielded by any agency that invokes it. The law enforcement agency must establish its mandate to enforce a particular law, and more importantly, that they are not unreasonably infringing on the rights of individuals guaranteed by the Constitution. Failure to establish both grounds renders the processing unnecessary and contrary to law.

[5] An Act Reorganizing And Modernizing The National Bureau Of Investigation (Nbi) And Providing Funds Therefor [NBI Reorganization and Modernization Act], Republic Act No. 10867, § 3 (2016).
[6] An Act Defining the Crime of Child Pornography, Prescribing Penalties Therefor and For Other Purposes [Anti-Child Pornography Act Of 2009] Republic Act No. 9775, § 20 (2009),
[7] An Act Instituting the Comprehensive Dangerous Drugs Act of 2002, Repealing Republic Act No. 6425, Otherwise known as the Dangerous Drugs Act of 1972, as Amended, Providing Funds Therefor, and for Other Purposes [Comprehensive Dangerous Drugs Act Of 2002] Republic Act No. 9165 (2002).

Section 2, Article III of the 1987 Philippine Constitution declares the inviolability of the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose, where a search warrant or warrant of arrest can only be issued upon finding of probable cause and by a court of competent jurisdiction. This provision has at its core the recognition of the right to privacy of individuals, and the guarantee that any limitations on this right is subject to the strictest scrutiny.

The right against unreasonable searches and seizures guards against the exercise of government of unbridled discretion in collecting, obtaining and using information relevant to individuals, for whatever purpose. The request for disclosure of **"school records"** as in this case**, "in connection with the investigation being conducted by this Bureau"** is not the same as the issuance of a search warrant. If it were so, then it would be akin to issuing a general search warrant through a mere letter-request, rendering the power of the NBI limitless to gather information, even in those cases where individuals have overriding privacy interests.

The NBI is not prohibited from making this request but neither is the school or institution obligated to disclose such information based only on the letter-request of NBI. The DPA should not be used to legitimize acts or omissions that violate fundamental freedoms. The DPA should always be interpreted in a manner consistent with the full respect for human rights enshrined in the Constitution.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-72

05 October 2018

[redacted]

Re: REVIEW OF CONSENT FORM

Dear [redacted],

We write in response to your request received by the National Privacy Commission (NPC) to review the National Kidney Transplant Institute's (NKTI) Consent Form template regarding its compliance with the Data Privacy Act of 2012.[1] Please see the template below with our comments:

NKTI Patient Consent Form	Remarks
Personal information required in the form: • Patient's Name (Last, First, Middle) • Sex • Age • Civil Status	When processing personal data, it should be considered that the processing shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[2] There is a need to review if all the listed personal information to be collected is necessary for the purpose. Note that some of the items being asked are sensitive personal information (age and civil status).[3]
CONSENT TO TREATMENT: □ I hereby authorize NKTI, its physicians and staff to perform diagnostic and treatment procedures that my/the patient's condition requires, except those procedures that need a specific written consent. I have been given an opportunity to ask questions and have them fully answered. □ Idonotauthorizeto[sic]theconditionsstatedabove and understand the consequences.	No comment

[1] 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).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(c) (2016).
[3] Data Privacy Act § 3(i)

NKTI Patient Consent Form	Remarks
ACCESS TO PATIENT'S INFORMATION: ▫ As long as my/the patient's identity is not disclosed, I hereby designate NKTI to be my/the patient's agent and authorize the latter to obtain information from other physicians, hospitals or clinics which are necessary for the patient's treatment and care while in NKTI. General information or data which may be gathered by NKTI during the course of my/the patient's treatment may be used for training purposes. I have been given an opportunity to ask questions and have them fully answered. ▫ I do not authorize to [sic] the conditions stated above and understand the consequences	Please clarify how NKTI can act as the agent of the patient and have the authority to obtain information from other physicians, hospitals, or clinics without disclosing the patient's identity. If the health information will be used for training purposes, consent which is specific for the purpose must be obtained. Therefore, we recommend that there be a separate provision for trainings and an enumeration of the types of training covered in the consent form. Additionally, please clarify the consequences of the patient choosing not to authorize NKTI.
CONSENT TO BE INCLUDED TO PATIENT REGISTRY: ☐ As long as my/the patient's identity is not disclosed, I hereby agree that all my information or data gathered during the course of my/the patient's treatment, may be accessed in compliance with the regulatory requirements of government agencies, including but not limited to DOH, and PhilHealth for statistical and research purposes. I have been given an opportunity to ask questions and have them fully answered. ☐ I do not authorize to [sic] the conditions stated above and understand the consequences.	To clarify, the processing of information necessary for the DOH and PhilHealth to fulfill their respective mandates is anchored on existing laws and regulations and not based on consent. Hence, a patient's consent may not be required in these instances. Nevertheless, the patient should be duly informed about the processing for such purposes, pursuant to the right of data subjects to be informed on whether personal data pertaining to him or her shall be, are being, or have been processed. Where processing is for statistical and research purposes, we understand that NKTI is mandated to conduct fact-finding investigations on kidney diseases and to report, publish and disseminate information on kidney and allied diseases, among others. Statistical data, if anonymized, is outside the scope of the DPA, provided that the anonymity of the individual data subject can be guaranteed.[4] Nonetheless, NKTI must still abide by existing rules and regulations on health research and research involving human participants such as the 2017 National Ethical Guidelines for Health and Health-Related Research. Finally, we wish to emphasize that the patient has the right to refuse to participate in the research or withdraw his or her participation therein without having to give any reason, and without penalty or loss of benefits to which he or she is entitled.[5]

[4] Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party of the European Commission provides an illustration on how a dataset would qualify as anonymous: "If an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data."

[5] Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical, Guidelines National Ethical Guidelines for Health and Health Related Research, 11-17 (2017)

NKTI Patient Consent Form	Remarks
AUTHORIZATION FOR RELEASE OF MEDICAL RECORDS: □ I hereby authorize NKTI to make a copy/ies of the result of my/the patient's clinical laboratory tests, radiological examination, and other medical records, procedures, treatment, etc. to be incorporated in my/the patient's records, except (if applicable) _____ and release such copy/ies to my/the patient's authorized representatives. I hereby hold NKTI free from all liability that may arise from the release of the said medical records. I have been given an opportunity to ask questions and have them fully answered. □ I do not authorize to [sic] the conditions stated above and understand the consequences	No comment
If you want to withdraw your consent to use your data or amend any information, submit your Letter of Intent to the Unit Head Nurse or Admitting Officer	We recommend that the contact details of the Unit Head Nurse, Admitting Officer, or the Data Protection Officer of NKTI be provided to the patient to give them an effective and efficient mode of reaching the concerned officers for any questions regarding the form.

In addition, in view of research being a part of the NKTI's mandate, you inquired about the acceptability of informing the patient that his or her personal information may be included in a research project in lieu of a separate consent portion.

This is not possible. While Presidential Decree No. 1832, which created the NKTI, did include research as part of your institution's mandate, the processing of personal and sensitive personal information for research is still subject to the requirements of existing laws and regulations governing research.

The Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012[6] (DPA) states that personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards, is outside of the scope of the law.[7] But this exemption from the requirements of the DPA is only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned, and does not extend to personal information controllers who remain subject to the requirements of implementing security measures for personal data protection.[8]

[6] 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).
[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).
[8] Id.

For health research and research involving human participants, we understand that the Department of Science and Technology - Philippine Council for Health Research and Development (DOST PCHRD) published the 2017 National Ethical Guidelines for Health and Health-Related Research (Guidelines), which was prepared by the Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical Guideline.

The said Guidelines state that an element of research ethics is informed consent, defined as a decision of a competent potential participant to be involved in research after receiving and understanding relevant information, without having been subjected to coercion, undue influence, or inducement.[9]

Further, the Guidelines require the consent of research participants, **to wit:**

> "For all research involving humans, the researcher shall obtain the voluntary informed consent of the prospective research participant. In the case of an individual who is incapable of giving or who has diminished capacity to give informed consent, the researcher must exert effort to obtain his or her assent and the consent of a legally authorized representative (LAR), in accordance with applicable laws."[10]

Similarly, under the Section 3(b) of the DPA, consent of the data subject is defined as 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.

In addition to the responses to your inquiries, we recommend the following to enhance the adherence of your consent form to the spirit of the general principles of data privacy:

- Provide introductory paragraphs which discusses the nature of NKTI as an institution;
- Modify the format of the consent form to simplify the consent statement, i.e. enumerate all purposes where consent is required, such as use of health information for training purpose, accreditation, inclusion in registry, etc.

[9] Philippine Health Research Ethics Board Ad Hoc Committee for Updating the National Ethical, Guidelines National Ethical Guidelines for Health and Health Related Research 11-12 (2017).
[10] Id.

    - A tick box for each item may be useful to ensure that the patient or data subject explicitly consented to each processing, provided that distinct purposes are separated and not bundled together.
    - Processes that do not require consent, such as use of personal data for reportorial requirements covered by existing laws and regulations may be incorporated in the hospital's privacy notice; and
- Consider translating the language used in the consent form.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-76

26 November 2018

[redacted]

Re: SUBMISSION OF PERSONAL DATA OF SEAFARERS TO THE MARITIME INDUSTRY AUTHORITY

Dear [redacted],

We write in response to your request for advisory opinion on whether your company, the Manila Shipmanagement & Manning, Inc. (Manship) may grant the request of the Maritime Industry Authority (MARINA) for certain personal data of seafarers, and whether the requested information is not covered by the Data Privacy Act of 2012[1] (DPA) as it falls under Section 4 (e) of the DPA, as "information necessary in order to carry out its statutorily mandated functions," and in light of Section 4.15, Rule I of the Implementing Rules and Regulations (IRR) of Executive Order No. 75, series of 2012[2] (E.O. No. 75).

We understand that Manship is a manning agency duly licensed by the Philippine Overseas Employment Administration (POEA) to engage in the recruitment and placement of qualified Filipino seafarers for vessels plying international waters and for related maritime activities. On the other hand, pursuant to E.O. No. 75 (2012)[3] as well as Republic Act (R.A.) No. 10635,[4] the MARINA is the authority responsible for the oversight and supervision of maritime education, training, and certification of

[1] 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).

[2] Office of the President, Designating the Department of Transportation and Communications (DOTC), Through the Maritime Industry Authority, as the Single Administration in the Philippines Responsible for Oversight in the Implementation of the 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, as Amended [E.O. No. 75] (Apr. 30, 2012).

[3] E.O. No. 75, § 1 - STCW Administration. The Department of Transportation and Communications (DOTC) through the MARINA shall exercise oversight and supervision over compliance with all qualification requirements and conditions under the STCW Convention, as amended, relating to maritime education, training and certification, subject to existing and applicable laws.

[4] An Act Establishing the Maritime Industry Authority (MARINA) as the Single Maritime Administration Responsible for the Implementation and Enforcement of the 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, as Amended, and International Agreements or Covenants Related thereto, Republic Act No. 10635 (2014).

seafarers in accordance with the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). In particular, Section 4(a) and (b) of RA No. 10635 provides:

> Section 4. Powers and Functions of the MARINA.—In addition to the mandate of the MARINA under Presidential Decree No. 474, as amended, and in order to carry out the provisions of this Act, the MARINA shall exercise the following powers and functions:
>
> > (a) Act as the single and central maritime administration for all purposes relating to compliance with the STCW Convention.
> >
> > (b) Administer and ensure the effective implementation of the STCW Convention; including all international conventions or agreements implementing or applying the same, as well as international maritime safety conventions or agreements that it seeks to promote compliance with.

In its letter dated 21 May 2018, the MARINA requested all manning agencies for certain information on seafarers who were awarded disability compensation, specifically:

a. Names;
b. Ranks;
c. Illnesses or injuries from which the disability claims arose;
d. Dates the cases for disability claims were filed; and
e. Dates the National Labor Relations Commission (NLRC), National Conciliation and Mediation Board (NCMB), or appellate court decisions awarding disability claims were promulgated.

As clarified by the MARINA, the request for information is the agency's response to the increase of cases being filed by injured and ill seafarers who allege that they are permanently disabled in order to claim large amounts of money intended as disability compensation. Such information shall help the MARINA prevent the issuance of STCW-related certificates to dishonest seafarers.

At the outset, we clarify that the provisions of the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[5] However, the law provides under Section 4 the particular types of information that are considered as special cases excluded from its scope and application.[6]

[5] Data Privacy Act of 2012, § 4.
[6] Id.

We affirm that the requested information by MARINA falls under Section 4 of the DPA, as expounded in Section 5 of its IRR, in particular, paragraph (d) which states:

> Section 5. Special Cases. **The Act and these Rules shall not apply to the following specified information**, **only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned**:
>
> xxx xxx xxx
>
> **Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function**, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act, Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
>
> xxx xxx xxx
>
> **Provided**, that **the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors**, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be **exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity**.[7] (Emphasis supplied)

As may be gleaned from the above provisions, however, the exemption is not absolute. The exclusion of such information from the scope of the law is limited to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function or activity. This means that while consent of the data subject is not required in the processing of such personal information, the non-applicability does not extend to the duties and responsibilities of an entity or organization as a personal information controller or personal information processor under the DPA.

[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 4 (2016).

We also note that Section 4.15, Rule I of the IRR of E.O. No. 75 provides that the MARINA has the power to "develop and enforce appropriate measures to prevent fraudulent acts and other unlawful practices involving the issuance of any certificates and endorsement in accordance with the requirements of the STCW Convention."

More importantly, paragraph 12 of Regulation I/2 of the Manila Amendments to the Annex to the 1978 International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (the STCW Convention)[8] (the Manila Amendments) decrees that, "Each Party shall ensure that certificates are issued only to candidates who comply with the requirements of this regulation." Furthermore, paragraphs 1 and 2 of Regulation I/5 therein states:

> Each Party **shall establish processes and procedures** for the impartial investigation of any reported incompetency, act, omission or compromise to security that may pose a direct threat to safety of life or property at sea or to the marine environment by the holders of certificates or endorsements issued by that Party **in connection with their performance of duties related to their certificates and for the withdrawal, suspension and cancellation of such certificates for such cause and for the prevention of fraud**.
>
> Each Party **shall take and enforce appropriate measures to prevent fraud and other unlawful practices involving certificates and endorsements issued**. (Emphasis supplied)

Accordingly, the MARINA has a mandated regulatory function, specifically on compliance with the duties under the STCW Convention and the Manila Amendments. MARINA must ensure that STCW-related certificates are issued only to qualified candidates. It is also evident that the MARINA has the obligation to prevent any fraudulent or unlawful practices involving the certificates that were issued.

Thus, the disclosure to the MARINA by Manship of the requested personal data of seafarers who were awarded disability compensation, may be considered as lawful processing under a special case in accordance with the DPA. Note, however, that the disclosure must be limited to the extent necessary to achieve the specific purpose**.**

In determining if the processing is necessary for the purpose, the UK

[8] International Maritime Organization, & International Conference on Training and Certification of Seafarers. STCW 1978: International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers, 1978 : with resolutions adopted by the International Conference on Training and Certification of Seafarers, 1978.

Information Commissioner's Office (ICO) produced a guide on the provisions of the Regulation (EU) 2016/679—which repeals the 1995 EU Directive from which the DPA is based on.

According to the guide, "necessary" means that the processing must be a targeted and proportionate way of achieving the purpose. An organization does not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.[9]

In the same manner, the principle of proportionality under the DPA requires a determination of what information are actually required for the fulfillment of a declared, specified, and legitimate purpose.[10]

According to MARINA , the purpose for requesting information is to prevent the issuance of STCW-related certificates to dishonest seafarers. As mentioned earlier, the dates for which the disability claims were filed by the seafarers are included in the requested information. These consist of all types of claims such as whether the disability claim is permanent or temporary, and whether the case filed is pending or promulgated.

To clarify, the MARINA, may process only those information which are necessary to carry out its mandates or functions, and shall be used for the specified purpose only. In this case, however, the disclosure of the fact of a pending case filed by a seafarer may not be necessary and proportionate to the purpose of helping the MARINA prevent the issuance of certificates to supposedly disabled seafarers.

Note further that such disclosure may result to a seafarer being profiled and/or blacklisted for simply filing a case, which might prevent seafarers with legitimate claims, from filing valid cases for disability claims. In the same manner, where the case takes a long time to be resolved, and where seafarer may have become already fit for work, the fact of a pending case may prevent him or her from seeking new employment or contract.

In which case, the information on cases which have not been decided with finality should not be considered as basis for non-issuance of STCW-related certificates, and even more, for determination of fraudulent acts. Indeed, there is a separate body that decides these claims. To label immediately those applying for a new contract where claims for

9 UK Information Commissioner's Office, Guide on the General Data Protection Regulation (GDPR): Public task, p. 76, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (last accessed Oct. 23, 2018).

10 Rules and Regulations Implementing the Data Privacy Act of 2012, § 18(c) (2016) - Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

disability (without distinction) are still pending, as possibly "fraudulent" may be overreaching.

One of the purposes of informational privacy is to prevent a person from being discriminated against based on unauthorized or unlawful processing of their personal data. In this regard, the information requested by the MARINA should relate to the requirements of certification and any other legally mandated functions.

In relation to this, one of the conditions for certification is medical fitness of a seafarer. Section 4(c)(5) of R.A. No. 10635 states that:

> (5) The MARINA shall coordinate with the DOH to ensure that the medical standards established to ascertain the medical fitness of seafarers are in accordance with the international conventions/ treaties and existing laws. For this purpose, the MARINA shall:
>
> > (i) Ensure that the medical examinations and issuance of medical certificates by the DOH accredited hospitals, medical clinics, and laboratories, including medical practitioners are in accordance with the standards prescribed by the STCW Convention; and
> >
> > (ii) Ensure that medical certificates are issued by a duly-qualified medical practitioner recognized by and accredited with the DOH, and for this purpose, a register of recognized medical practitioners shall be maintained and made available to seafarers, shipping companies and State parties to the STCW Convention.[11]

Furthermore, the International Labour Organization and International Maritime Organization developed a guideline aimed at providing maritime administrations with an internationally recognized set of criteria for use by competent authorities either directly or as the basis for framing national medical examination standards that will be compatible with international requirements.[12] According to part IV of the guidelines:

> The medical certificate is neither a certificate of general health nor a certification of the absence of illness. It is a confirmation that the seafarer is expected to be able to meet the minimum requirements for performing the routine and emergency duties specific to their post at sea safely and effectively during the period of validity of

[11] R.A. No. 10635, § 4(c)(5)

[12] International Labour Organization and International Maritime Organization. (2013). Guidelines on the medical examinations of seafarers, p.7 (available at: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/normativeinstrument/wcms_174794.pdf)

> the medical certificate. Hence, **the routine and emergency duties must be known to the examining medical practitioner, who will have to establish, using clinical skills, whether the seafarer meets the standards for all anticipated routine and emergency duties specific to their individual post and whether any routine or emergency duties need to be modified to enable them to be performed safely and effectively.**[13] (Emphasis Supplied)

In view of the aforementioned, it is clear that the MARINA has a responsibility to guarantee that all medical certificates issued are in accordance with the standards established by the STCW Convention. Moreover, compliance with the STCW Convention requires the reliable expertise of a medical practitioner who shall ultimately determine the medical fitness of a seafarer.

Clearly from the foregoing, the effective evaluation of applications for STWC-related certificates submitted by seafarers especially in order to prevent fraud, is not solely dependent on the requested information. This means that the MARINA may still achieve its purpose through other means such as, but not limited to, improving their policies and procedures in the issuance of such certificates.

We take time to emphasize that the right to privacy of seafarers in terms of their medical examinations is also recognized under part VII of the Guidelines developed by the International Labour Organization and International Maritime Organization, which states:

> VII. Right to privacy
> All persons involved in the conduct of medical examinations, including those who come into contact with medical examination forms, laboratory results and other medical information, should ensure the right to privacy of the examinee. Medical examination reports should be marked as confidential and so treated, and all medical data collected from a seafarer should be protected. **Medical records should only be used for determining the fitness of the seafarer for work and for enhancing health care; they should not be disclosed to others without prior written informed consent from the seafarer. Personal medical information should not be included on medical certificates or other documents made available to others following the medical examination.** The seafarer should have the right of access to and receipt of a copy of his/her personal medical data.[14] (Emphasis Supplied)

[13] Id., p.9.

[14] International Labour Organization and International Maritime Organization. (2013). Guidelines on the medical examinations of seafarers, p.13 (available at: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/normativeinstrument/wcms_174794.pdf)

Taking into account the discussions, only adjudicated cases where an award for personal disability has been granted with finality may be disclosed, with due notice to seafarer. As to the disclosure of additional information, the MARINA must be able to justify the necessity and proportionality of such disclosure in fulfilling its mandate. The justification must have considered all other less invasive methods in order to obtain the same outcome or purpose.

We trust that the MARINA is aware that it is still subject to the requirements of the DPA, such as upholding the rights of the data subjects and implementing organizational, physical and technical security measures for the protection of personal data.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Deputy Privacy Commissioner
Officer-In-Charge

ADVISORY OPINION
NO. 2018-77

25 October 2018

[redacted]

Re: CONGRESSIONAL REQUEST FOR LISTS OF BENEFICIARIES OF THE PANTAWID PAMILYANG PILIPINO PROGRAM (4Ps) AND THE SOCIAL PENSION FOR INDIGENT SENIOR CITIZENS PROGRAM

Dear [redacted],

We write in response to your request for an advisory opinion which sought clarification on the possible data privacy concerns regarding the request for information from the Chairperson of the Committee on Appropriations of the House of Representatives. The request states in part as follows:

> "In the performance of the oversight function of Congress through the House Committee on Appropriations, this representation respectfully requests from your good office the list of beneficiaries of the following DSWD programs:
>
> 1. Pantawid Pamilyang Pilipino Program (4Ps)
> 2. Social Pension for Indigent Senior Citizens Program."

We understand that both the 4Ps and the Social Pension for Indigent Senior Citizens Program are government programs under the DSWD aimed at providing assistance to indigents. Both programs, in processing personal information of beneficiaries, are covered by the Data Privacy Act of 2012[1] (DPA).

[1] 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).

1. Would the names of the beneficiaries be considered as personal information or sensitive personal information?

The names of the beneficiaries are considered as personal information, defined under the DPA as 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.[2] It is not sensitive personal information. The DPA under Section 3(l) provides an enumeration of what constitutes sensitive personal information, such as a person's race, marital status, age, health and educations records, social security numbers, among others.

2. If the DSWD is asked to provide a sorted list, e.g. sorted by congressional district, would that constitute another field of information? If so, would such additional information be considered personal information or sensitive personal information?

The sorted list showing congressional district would constitute another field of information, as the list would now indicate name and address, albeit limited to district, of the data subject. The information is considered personal information and not sensitive personal information.

3. Assuming the names and other information of beneficiaries are considered merely "personal information" and not "sensitive personal information", under Section 12(c) of the DPA, the same may be processed when "The processing is necessary for compliance with a legal obligation to which the personal information controller is subject." In this instance, would the oversight function of Congress qualify as a "legal obligation" of the DSWD?

Congressional oversight embraces "all activities undertaken by Congress to enhance its understanding of and influence over the implementation of legislation it has enacted. Clearly, oversight concerns post-enactment measures undertaken by Congress: (a) to monitor bureaucratic compliance with program objectives, (b) to determine whether agencies are properly administered, (c) to eliminate executive waste and dishonesty, (d) to prevent executive usurpation of legislative authority, and (d) to assess executive conformity with the congressional perception of public interest."[3]

We refer to the Rules of the House of Representatives[4] which declares

[2] Id. 3 (g).
[3] Abakada Guro Party List v. Purisima, G.R. No. 166715 (2008), citing Macalintal v. COMELEC, 453 Phil. 586 (2003).
[4] House of Representatives, Rules of the House of Representatives 16th Congress, as adopted by the 17th Congress, available at http://www.congress.gov.ph/download/docs/hrep.house.rules.pdf (last accessed 2 October 2018).

that "efficient and effective access to and dissemination of appropriate and accurate information are imperative in lawmaking."[5] Further, the said rules state that "Committees shall have oversight responsibilities to determine whether or not laws and programs addressing subjects within their jurisdictions are being implemented and carried out in accordance with the intent of Congress and whether or not they should be continued, curtailed, or eliminated."[6]

In addition, the rules provide that committees shall review and study on a continuing basis, or upon order of the House:

a. the application, administration, execution, and effectiveness of laws and programs addressing subjects within their respective jurisdictions;
b. the organization and operation of national agencies and entities having responsibilities for the administration and execution of laws and programs addressing subjects within their respective jurisdictions; and
c. any conditions or circumstances that may indicate the necessity or desirability of enacting new or additional legislation addressing subjects within their respective jurisdictions.[7]

Note that Section 12 of the DPA provides for the criteria for lawful processing of personal information. Included among these is the criterion relating to the mandate of public authorities, i.e. when "processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or **to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate**."[8]

In view of the foregoing, the request for information and processing to be done by the Committee on Appropriations may be founded on the fulfillment of the mandate of the said Committee exercising its oversight function.

4. Again assuming the names and other information of beneficiaries are considered merely "personal information" and not "sensitive personal information", under Section 12(f) of the DPA, the same may be processed when "The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed." In this instance, would the "oversight function

[5] Id. Declaration of Principles and Policies
[6] Id. Rule IX, § 26.
[7] Id.
[8] Data Privacy Act of 2012, § 12 (e).

of Congress qualify as a "legitimate interest" of the Congress?

The processing performed by the government should always be anchored on the Constitution, or mandated by a law, rule or regulation. Hence, legitimate interest of government should have statutory or constitutional basis.

However, as discussed above, the disclosure of information by the DSWD to the Committee may be based on the fulfillment of the functions of a public authority under Section 12 (e) of the DPA.

5. Assuming the names and other information of beneficiaries are considered merely "sensitive personal information" (and not merely "personal information"), under Section 13(f) of the DPA, the same may be processed when "The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority." In this instance, would the Committee on Appropriations of the House of Representatives qualify as a "government or public authority"?

As discussed, the names and addresses of beneficiaries are personal information and not sensitive personal information. However, should such list contain additional information of the beneficiaries, i.e. marital status, age, social security numbers, tax identification numbers, etc., these are then considered as sensitive personal information, and the applicable criteria for lawful processing may be Section 13(b) where processing is provided for by existing laws and regulations and/or Section 13(f) processing concerns such personal information provided to government or public authority.

6. In sum, and considering all of the foregoing, would it be lawful for the DSWD to grant the request mentioned above, and provide the Committee on Appropriations of the House of Representatives with the lists of beneficiaries of the 4Ps and of the Social pension for Indigent Senior Citizens Program?

DSWD may grant the request of the Committee on Appropriations of the House of Representatives pursuant to the oversight function cited and the criteria for lawful processing of personal information as discussed above.

However, DSWD should also consider the principle of proportionality,

whereby the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

We note that the 2018 General Appropriations Act (GAA) Special Provisions for the 4Ps and Social Pension for Indigent Senior Citizens Program merely require DSWD to "submit its quarterly reports on the financial and physical accomplishments with electronic signature to the DBM, through the unified reporting system, and to the Speaker of the House of Representatives, the President of the Senate of the Philippines, the House Committee on Appropriations and the Senate Committee on Finance..."

Therefore, there is a need to determine if statistics or aggregated data will suffice for the oversight function of the Committee on Appropriations of the House of Representatives instead of requiring individual level data.

We underscore that the interpretation of any provision of the DPA must be in a manner mindful of the rights and interests of the data subject.[9] Processing operations performed about vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor,[10] require special protection.[11]

Further, the risk to the rights and freedoms of persons that may result from personal data processing which could lead to physical, material or non-material damage, i.e. where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles,[12] should be considered as well.

Should aggregated data be insufficient for the purpose, the House of Representatives should provide information why the specific personal information requested is necessary in relation to its declared purpose. Where the House of Representatives collects and processes this

[9] Data Privacy Act of 2012, § 38.

[10] National Privacy Commission, Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making, Circular No. 17-01 [NPC Circular 17-01], § 5 (c) (3) (July 31, 2017).

[11] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Item III (B)(a)(7), 4 April 2017, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, (last accessed 12 Oct 2018).

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016), Recital 75.

information from the DSWD, the House will be bound by its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies and NPC Circular No. 16-02 - Data Sharing Agreements Involving Government Agencies.

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.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) LEANDRO ANGELO Y. AGUIRRE
Officer-in-Charge and
Deputy Privacy Commissioner
for Data Processing Systems

ADVISORY OPINION
NO. 2018-78

16 October 2018

[redacted]

Re: DISCLOSURE OF PERSONAL DATA FOR THE DEPARTMENT OF LABOR AND EMPLOYMENT'S AUDIT OF EMPLOYERS

Dear [redacted],

We write in response to your letter request for advisory opinion wherein you sought clarification on whether the Convergys Group, namely, Convergys Philippines, Inc., Convergys Singapore Holdings Inc. – ROHQ, Convergys Malaysia (Philippines) Sdn. Bhd. – Philippine Branch, and Encore Receivable Management, Inc. – Philippine Branch:

a) can provide government agencies which have audit powers, the personal information and sensitive personal information of its employees; and
b) if the aforesaid sharing and disclosure of the same will not require the consent of and/or prior notice to its employees.

From your letter, we understand that DOLE requests for documents which contain personal and sensitive personal information of your employees, including:

a) roster of employees, status of employment, date of hire, and wage rate;
b) pay slips of employees, which contain their name, wage received, and other financial information such as loan details;
c) records of leave benefits, which may contain leave benefits pertaining to maternity leaves and violence against women leaves;
d) list of foreign officials currently employed by the company, their nationality, nature of employment, status of stay in the Philippines, copies of their Alien Employment Permit,

which contain their name, nationality and Tax Identification Number (TIN), among others, and copies of their Alien Card Registrations, which contains their name, nationality, civil status, sex, and date of birth; and

e) contracts with various vendors, which contain names, contact information and other personal information such as TIN of the signatories.

You mentioned as well that while you recognize the Department of Labor and Employment's (DOLE) authority to audit employers, you also need to ensure that you comply with both their requests and the requirements of Data Privacy Act of 2012[1] (DPA). Furthermore, you are concerned with similar situations that may arise from your transactions with other government agencies such as the Social Security System and Bureau of Internal Revenue. Hence, you wanted an opinion on the extent of information that you may provide to these government agencies.

Lawful criteria for processing of personal data; general data privacy principles

The DPA applies to the processing of all types of personal information[2], sensitive personal information[3], and privileged information[4] (collectively referred to as personal data) and to any natural and juridical person involved in the processing thereof, including government agencies. The collection, disclosure or any type of processing of the requested personal data by DOLE fall within the ambit of the law, which dictates the requirements that must be complied with.

Sections 12 and 13 of the DPA lay down the specific criteria which must be met for the lawful processing of personal information and sensitive personal information, respectively. In order to authorize any processing of personal data, a personal information controller (PIC) must adhere to all the requirements established by the DPA. Sections 12(e) and 13(b) provide:

---

[1] 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).

[2] Id. § 3 (g) - 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.

[3] Id. § 3 (l) - Sensitive personal information refers to personal information:
About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;
Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
Specifically established by an executive order or an act of Congress to be kept classified.

[4] Id. § 3 (k) - Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

"SECTION 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

xxx

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate;

xxx

SECTION. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(b) The processing of the same is provided for by existing laws and regulations; Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;"

As set out in the Administrative Code of 1987,[5] the DOLE is mandated to be the primary policy-making, programming, coordinating and administrative entity of the Executive Branch of the government in the field of labor and employment.[6] It shall assume primary responsibility for:

(1) The promotion of gainful employment opportunities and the optimization of the development and utilization of the country's manpower resources;

(2) The advancement of workers' welfare by providing for just and humane working conditions and terms of employment;

(3) The maintenance of industrial peace by promoting harmonious, equitable, and stable employment relations that assure equal protection for the rights of all concerned parties.[7]

[5] Office of the President, Instituting the "Administrative Code of 1987," Executive Order No. 292 [Administrative Code of 1987] (July 25, 1987).
[6] Id. Book IV, Title VII, Chapter 1, § 2.
[7] Ibid.

Furthermore, the DOLE has the following powers and functions set out by the same law, **viz**:

> "SECTION 3. Powers and Functions.—The Department of Labor and Employment shall:
>
> (1) Enforce social and labor legislation to protect the working class and regulate the relations between the worker and his employer;
>
> (2) Formulate and recommend policies, plans and programs for manpower development, training, allocation, and utilization;
>
> (3) Recommend legislation to enhance the material, social and intellectual improvement of the nation's labor force;
>
> (4) Protect and promote the interest of every citizen desiring to work locally or overseas by securing for him the most equitable terms and conditions of employment, and by providing social and welfare services;
>
> (5) Regulate the employment of aliens, including the enforcement of a registration or work permit system for such aliens, as provided for by law;
>
> (6) Formulate general guidelines concerning wage and income policy;
>
> (7) Recommend necessary adjustments in wage structures with a view to developing a wage system that is consistent with national economic and social development plans;
>
> (8) Provide for safe, decent, humane and improved working conditions and environment for all workers, particularly women and young workers;
>
> (9) Maintain a harmonious, equitable and stable labor relations system that is supportive of the national economic policies and programs;
>
> (10) Uphold the right of workers and employers to organize and promote free collective bargaining as the foundation of the labor relations system;

(11) Provide and ensure the fair and expeditious settlement and disposition of labor and industrial disputes through collective bargaining, grievance machinery, conciliation, mediation, voluntary arbitration, compulsory arbitration as may be provided by law, and other modes that may be voluntarily agreed upon by the parties concerned; and

(12) Perform such other functions as may be provided by law."

In line with its mandate, powers and functions, the DOLE promulgated Department Order No. 183, Series of 2017, known as the Revised Rules on the Administration and Enforcement of Labor Laws Pursuant to Article 128 of the Labor Code, as Renumbered[8] (D.O. 183) which aims to further strengthen the implementation of the visitorial and enforcement powers of the Secretary of Labor under the Labor Code.[9] Verily, Article 128 of the Labor Code provides in part:

> "The Secretary of Labor and Employment or his duly authorized representatives, including labor regulation officers, shall have access to employer's records and premises at any time of the day or night whenever work is being undertaken therein, and the right to copy therefrom, to question any employee and investigate any fact, condition or matter which may be necessary to determine violations or which may aid in the enforcement of this Code and of any labor law, wage order or rules and regulations issued pursuant thereto."[10]

Given the foregoing, the DOLE is indeed duly authorized to audit employers, and collect, obtain and process the requested information as necessary for the implementation of its mandated powers and functions. Thus, the requested personal data of your employees in your custody may be disclosed to DOLE without the consent of your employees.

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 the facts.

---

[8] Department of Labor and Employment, Revised Rules on the Administration and Enforcement of Labor Laws Pursuant to Article 128 of the Labor Code, as Renumbered [D.O. 183, s. 2017], (October 18, 2017).

[9] A Decree Instituting a Labor Code Thereby Revising and Consolidating Labor and Social Laws to Afford Protection to Labor, Promote Employment and Human Resources Development and Insure Industrial Peace Based on Social Justice, Presidential Decree No. 442, as amended [Labor Code], (May 1,1974).

[10] Id. § 128. Underscoring supplied.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-80

26 November 2018

[redacted]

Re: VIEWING AND/OR RELEASE OF CCTV FOOTAGES

Dear [redacted],

We write in response to your inquiry which sought to clarify whether a joint viewing or releasing of a copy of your closed-circuit television (CCTV) camera footages to a customer is in accordance with the provisions stated of the Data Privacy Act of 20121 (DPA), its Implementing Rules and Regulations (IRR) and relevant issuances of the National Privacy Commission (NPC).

In your letter, you stated that you are in the business of operating restaurants. Due to the traffic of customers coming in and going out of the establishment, the installation of a CCTV camera is indeed useful in monitoring and securing your daily operations. You also mentioned that a customer and her legal counsel sent a letter request seeking for a joint viewing and/or provision of a copy of the footages, to aid in pursing the individual/s liable for the loss of the customer's cellular phone.

A CCTV is a camera surveillance system that captures images of individuals or information relating to individuals.2 If the camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from the footage. 3 Thus, the footage and images are considered personal information and the provisions of the DPA will apply.

Given that the entity is processing4 personal data, it is bound to comply with the duties and responsibilities of a personal information controller

[1] 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).

[2] See: Office of the Privacy Commissioner (New Zealand). Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations (2009), available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf (last accessed Oct. 16, 2018).

[3] See: Office of the Information Commissioner (Queensland). Camera Surveillance and Privacy (2009), available at https://www.oic.qld.gov.au/__data/assets/pdf_file/0010/28099/guideline-camera-surveillance-and-privacy.pdf (last accessed Oct. 16, 2018).

[4] Data Privacy Act of 2012, § 3 (j).

(PIC)5, including the adherence to the principles of transparency, legitimate purpose and proportionality.6 It should have informed and clearly notified the customers and the public in general, through a privacy notice or prominent signs at the entrance of the surveillance system's zone, that the establishment is being monitored by a CCTV camera, how data is being collected and its definite purpose for installing such equipment, as well as the relevance of the footages to be obtained in achieving or fulfilling the specified purpose of surveillance.7

Moreover, as a PIC, the entity is bound to implement reasonable and appropriate organizational, physical, and technical measures to protect the personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.8 It must issue a guidelines or policies on how footages can be viewed, or acquired, who are authorized to access, when data can be shared or transferred and the corresponding retention period.

Given the crucial responsibility to secure personal information, the purpose and extent of disclosure requested by the customer and her counsel must be thoroughly evaluated based on the criteria for lawful processing of personal information in Section 12 of the DPA, to wit:

a. The data subject has given his or her consent;
b. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
d. The processing is necessary to protect vitally important interests of the data subject, including life and health;
e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
f. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

[5] Id. § 3 (h).
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 §17 (2016).
[7] Id. § 18.
[8] Data Privacy Act of 2012, § 20.

Based on the provision above, the viewing or disclosure of footages to the customer and her legal counsel, for identification of the person liable for the loss of personal property, can be considered as processing necessary for the legitimate interests of the third party or parties to whom the data is disclosed.

To determine if there is "legitimate interest" in processing personal information, PICs must consider the following: 9

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PICs or third party, considering the likely impact of the processing on the data subjects.

In view of the foregoing, the viewing and/or disclosure of footages should be limited to the following:

1. Specific date of the incident;10
2. Particular time and duration of stay of the data subject in the establishment;11
3. If there are several CCTV cameras being operated, viewing only of the camera positioned at the precise location of the data subject during the incident;12 and
4. Viewing only by the data subject, and other persons permitted by the data subject.13

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated. Please be advised that the NPC may issue further guidelines on this matter.

[9] See generally, Data Privacy Act of 2012, § 12(f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ (last accessed on June 11, 2018).
[10] Supra note 3.
[11] Id.
[12] Id.
[13] Id.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

ADVISORY OPINION
NO. 2018-81

26 November 2018

[redacted]

Re: ACCESS TO MEDICAL RECORDS IN CR-DR SYSTEM

Dear [redacted],

We write in response to your letter regarding the access, use and destruction of medical records of patients stored in a Computerized Radiography- Digital Radiography (CR-DR) system in relation to the provisions of the Data Privacy Act of 2012 (DPA).1

In 2017, Western Visayas Medical Center (WVMC) requested a Special Audit from the Commission on Audit (COA) and pending the result thereof, held in abeyance the amount due to JOSMEF Enterprises (JOSEMEF) for the provision of equipment and system to enhance WVMC's radiography system. Because of this, JOSMEF filed a complaint before the Department of Health (DOH) against the hospital for nonpayment. At the same time, they did not allow the access of hospital personnel to the records of patients contained in the CR-DR System which is owned by JOSMEF. Hence, this inquiry as to whether JOSMEF should allow WVMC access to the data of patients in the CR-DR system, to copy the files, and to require JOSMEF to delete the files from the system should JOSMEF pull out the unit from the hospital.

We note that the concerns raised in this advisory may involve legal issues outside the scope of the DPA, particularly as it relates to interpretation of contracts, contractual obligations between the parties, and adjudication of rights. As we understand, WVMC entered into a joint undertaking with JOSMEF in April 2016 for the latter to provide the former with the equipment and system for the enhancement of its radiography system.

[1] 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).

We are not in a position to determine the nature of this joint undertaking as this involves not just the legal documents made available to the Commission but a determination of the factual circumstances relevant to the agreement.

Given this, we will only discuss the general principles relevant to this case in so far as such issues may relate to the DPA.

Personal Information Controller and Personal Information Processor

Given the issue at hand, it is vital to determine the relationship between the two entities in relation to the processing of patient data in the CR-DR System. The rights and obligations of the parties would be different depending on their relationship, particularly if they are joint personal information controllers, or if their relationship is one between a personal information controller and personal information processor. A personal information controller (PIC) refers to the individual or organization who controls how personal data – which includes health records -- are being collected, used, stored, or otherwise processed.2 On the other hand, a personal information processor (PIP) refers to any individual or organization processing personal information for the PIC as part of an outsourcing contract or similar agreement.3

If it were the case that the agreement is strictly for JOSMEF to install, configure and maintain the CR-DR system in accordance with the instructions of WVMC, and for this limited purpose have access to the personal data of patients of WVMC, then WVMC would be considered as the PIC and JOSMEF as the PIP.

It bears stressing that a PIP, as such, does not have a right to control the collection, holding, processing, or use of personal information of data subjects. PIPs must process personal data only in accordance with instructions from or under an agreement with a PIC. Where a PIP performs its own operations upon personal data, such as exercising control over its storage, use or retrieval, the PIP may already be considered a PIC. This means that the PIP will be subjected to all the obligations of a PIC under the DPA, including adherence to the data privacy principles of transparency, legitimate purpose and proportionality. Where a PIP processes personal data for its own purposes, including the retention of records, the PIP may risk liability for unauthorized processing and

[2] Data Privacy Act of 2012, § 3 (h).
[3] Id, § 3 (i).

other DPA violations if the processing is done without consent from data subjects or authority from law.

Principle of Accountability

The principle of accountability is articulated in Section 21 of the DPA, which provides:

> Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
>
> (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. xxx

Furthermore, Section 14 of the DPA provides that in case the PIC subcontracts the processing of personal information, the PIC is responsible for ensuring that proper safeguards are in place for data protection. This same section also provides that a personal information processor shall comply with all the requirements of the DPA and other applicable laws.

One of the guarantees of the Data Privacy Act is the protection of the rights of data subjects. Under the DPA, the data subject is entitled to the right of reasonable access to contents of his or her personal information that have been processed. In this case, this involves ensuring that patients can exercise their right to access medical information relating to them.

In the ordinary course of things, the PIC directly responds to the access requests of data subjects, with the cooperation and assistance of the PIP. The failure of the PIC to uphold the right to access of data subjects, without just and valid grounds, may make the PIC accountable to the data subject. This obligation is similarly imposed on PIPs considered as PICs because they control or determine the means and purposes of processing of personal data.

While the obligation to respond to data subjects rests primarily with the PIC, the PIP to whom a PIC has outsourced the processing of personal data should keep in mind its separate obligation to comply with all the

requirements of the DPA. Thus, a PIP would still need to uphold the rights of data subjects. This requirement may be complied with by cooperating and coordinating with the PIC in ensuring that data subjects are able to exercise their rights. Under special circumstances, where the PIC is unable to respond to access requests from data subjects, the PIC may instruct the PIP to put in place mechanisms to directly respond to access requests of data subjects, in order to remain mindful of the rights and interests of the individual about whom personal information is processed.

In this case, this is especially important because denial of access to medical information may impair the rights of patients as data subjects. A medical record is critical to patient care and the restriction or delay of access may have significant implications on the health and life of patients.

While we make no determination on the rights of the parties, the nature of their agreement, or possible liabilities, what is clear is that patients should not be denied access to their medical information. This is part of their rights as data subjects, which must be upheld by both PICs and PIPs.

This opinion is rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Deputy Privacy Commissioner
Officer-In-Charge

ADVISORY OPINION
NO. 2018-83

26 November 2018

[redacted]

Re: COLLECTION OF HEALTH INFORMATION BY THE DEPARTMENT OF HEALTH

Dear [redacted],

We write in response to your request for an advisory opinion regarding processing of health information by the Department of Health (DOH) related to its conduct of disease surveillance, epidemic investigation, contact tracing, survey research and disease registry, among others, at the national and regional level as part of its mandate aimed at providing accurate and complete health information for its policies, programs, and interventions.

During a clarificatory meeting, we were informed about the difficulty that the DOH encounters when collecting health information from healthcare providers[1] due to apprehensions on the implications of the Data Privacy Act of 2012 (DPA).[2] We understand that there are some healthcare providers claiming that the DOH is collecting excessive amounts of personal information. You have explained that collection of both personal information and sensitive information is necessary to minimize double counting of reportable health information, and allows for epidemic investigation and contact tracing when required by the circumstances. Monitoring of disease conditions, health outcomes and effects of intervention also require personal data.

[1] Department of Health (DOH)-Department of Science and Technology (DOST)-Philippine Health Insurance Corporation (PhilHealth) Joint Administrative Order (JAO) 2016-0002, Annex 2.0, Definition of Terms, health care provider – a health care institution devoted primarily to management, treatment and care of patients OR a health care professional, who is any doctor of medicine, nurse, midwife, dentist, or other health care practitioner.

[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).

The DPA is not meant to prevent government institutions from processing personal data when necessary to fulfill their mandates. Rather, it aims to protect the right to information privacy while ensuring free flow of information. What the DPA does is to promote fair, secure, and lawful processing of such information. In this case, the DPA does not prohibit the DOH from collecting and processing personal data for purposes necessary to its mandate, with the concomitant responsibility of complying with the requirements of the DPA, its Implementing Rules and Regulations (IRR), and other issuances of the National Privacy Commission (NPC).

In the meeting between representatives of the DOH and the NPC, the constitutional and statutory mandate of the DOH were discussed in relation to its personal data processing activities. The Philippine Constitution mandates the protection and promotion of the right to health of the people and the adoption of an integrated and comprehensive approach to health development.[3] This mandate is exercised by the DOH as the government agency primarily responsible for the formulation, planning, implementation, and coordination of the policies and programs in the field of health.[4] With this, the DOH processes personal data in order to perform the following functions as mandated in the Revised Administrative Code of 1987:

1. Define the national health policy and formulate and implement a national health plan within the framework of the government's general policies and plans, and present proposals to appropriate authorities on national issues which have health implications;
2. Provide for health programs, services, facilities and other requirements as may be needed, subject to availability of funds and administrative rules and regulations;
3. Coordinate or collaborate with, and assist local communities, agencies and interested groups including international organizations in activities related to health;
4. Administer all laws, rules and regulations in the field of health, including quarantine laws and food and drug safety laws;
5. Collect, analyze and disseminate statistical and other relevant information on the country's health situation, and require the reporting of such information from appropriate sources;
6. Propagate health information and educate the population on important health, medical and environmental matters which have health implications;
7. Undertake health and medical research and conduct training in support of its priorities, programs and activities;

[3] Phil. Const. art. 2, § 15, art. 13, § 11.
[4] Instituting the Administrative Code of 1987 [Administrative Code of 1987], Executive Order 292, Title IX, § 2 (1987).

8. Regulate the operation of and issue licenses and permits to government and private hospitals, clinics and dispensaries, laboratories, blood banks, drugstores and such other establishments which by the nature of their functions are required to be regulated by the Department;
9. Issue orders and regulations concerning the implementation of established health policies; and
10. Perform such other functions as may be provided by law.[5]

In addition, the DOH, through its offices and staff support services, also has the mandate to conduct studies and research on various disease conditions, to fulfill health intelligence services, and to maintain effective and comprehensive health information systems.[6]

The DPA should not be an obstacle to the collection and further processing of personal data by DOH as long as the same is necessary for the fulfillment of its mandate. In this case, the use of personal information and sensitive personal information for policy development, monitoring of health programs, and provision of better health care services is recognized as being necessary for DOH to perform its functions.

The processing of personal data by DOH finds support in the DPA. The DOH is a public authority performing regulatory functions, and is permitted to process personal data to the extent necessary for the fulfillment of these functions. [7] DOH also processes personal data for research purpose.[8] Furthermore, DOH may also rely on the provisions of the DPA in Sections 12 and 13 providing the criteria for lawful processing of personal information and sensitive personal information, respectively. For instance, Section 13 provides that the processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

> xxx
>
> (a) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

[5] Id. Title IX, § 3.
[6] Id. Title IX, §§10, 13-15
[7] Data Privacy Act of 2012, § 4.
[8] Data Privacy Act of 2012, § 4.

(b) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

xxx

(c) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[9]

While the DOH may have lawful basis in processing personal and sensitive personal information, it must, however, comply with its obligations as a personal information controller under the DPA, its IRR and related issuances. In processing personal data, DOH should be mindful of the rights of data subjects and ensure that it adheres to the principles of transparency, legitimate purpose and proportionality.[10] The basis of its processing should be documented and made known to healthcare providers subject to the DOH reporting requirements. For their part, these healthcare providers should, in turn, inform their data subjects of the fact of such processing by the DOH and the scope, nature, extent, purpose, and basis for the same.

These reporting requirements should be reviewed to ensure that personal data being processed is adequate and not excessive in relation to the purposes for which they are collected and processed.[11] There should also be existing procedures for data subjects to exercise their rights, and appropriate organizational, physical and technical safeguards for data protection.

The DOH should consider NPC Advisory No. 2017-03 on the Guidelines on Privacy Impact Assessments in order to systematically address the obligations previously mentioned. As a government agency, the DOH should also consider NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies and NPC Circular No. 16-02 regarding the execution of a data sharing agreement between the DOH and the different healthcare providers, as may be necessary in certain circumstances.

This opinion is rendered based on the information provided. Additional information may change the context of the inquiry and the appreciation of the facts.

[9] Data Privacy Act of 2012, § 13.
[10] Data Privacy Act of 2012, § 11.
[11] Data Privacy Act of 2012, § 11 (d).

For you reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Deputy Privacy Commissioner
Officer-In-Charge

ADVISORY OPINION
NO. 2018-84

28 November 2018

[redacted]

Re: COMPUTER MONITORING

Dear [redacted],

We write in response to your inquiry on whether secret surveillance on an employee's computer activities through the installation of a monitoring software to record keystrokes and take random snapshot of computer screen is prohibited under the Data Privacy Act of 2012[1] (DPA).

We wish to limit the succeeding discussion on an employer's act of monitoring the employees at the workplace, specifically, monitoring employee activities when he or she is using an office-issued computer.

Scope of the DPA; general data privacy principles

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Where the computer monitoring results in the collection of personal, sensitive personal or privileged information (collectively, personal data) of employees, the employers are engaged in processing personal data, and thus, covered by the provisions of the DPA.

Monitoring employee activities when he or she is using an office-issued computer may be allowable under the DPA, provided the processing falls under any of the criteria for lawful processing of personal data under Sections 12 and/or 13 of the law.

Employers, as personal information controllers (PICs), shall ensure that the processing complies with the general data privacy principles of transparency, legitimate purpose and proportionality.

[1] 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).

First, it is incumbent upon the employer to determine the purpose/s of computer monitoring, which must not be contrary to law, morals, or public policy.[2] Some possible legitimate purposes of computing monitoring are as follows: management of workplace productivity, protection of employees, business assets, intellectual property or other proprietary rights, prevention of vicarious liability where the employer assumes legal responsibility for the actions and behavior of employees,[3] and the like.

Alongside the determination of the purpose of processing, the employer shall assess the proportionality of the information collected, and the ways and means of processing. This principle directs the employer to process information that is adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.[4]

The methodology of data collection should likewise be proportional to the achievement and fulfillment of the purpose of the employer. Thus, personal data of the employees shall only be collected, used and stored by the employer, through computer monitoring, if the purpose sought to be achieved cannot be fulfilled by any other less privacy intrusive means.

In all cases, the employer is duty-bound to inform and notify the data subjects of the nature, purpose, and extent of computer monitoring and processing when using office-issued computers.[5] Moreover, the employer must issue a policy or set of guidelines on the use of company-issued devices and equipment.

Recommendation

"Secret surveillance" as you mentioned is frowned upon. Regardless of the legitimate purpose of processing, is the duty of the employer to explain the conduct of computer monitoring to the employees, the specific purpose, scope and actual method of monitoring, security measures to protect personal data, as well as the procedure for redress in cases where the rights of the employee as a data subject are violated.

The use of a software that records the keystrokes of the user and/or takes random photos of the computer screen seems to be an excessive and disproportionate mechanism in monitoring employees. Unless the declared purpose of computer monitoring necessitates and justifies the use of such extreme measure, the same should not be carried out.

---

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (b) (2016).
[3] Privacy Commissioner for Personal Data, Hong Kong, Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016), available at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_ Personal_Data_Privacy_At_Work_revis_Eng.pdf (last accessed Oct. 26, 2018)
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).
[5] Id. § 18 (a).

Every employer conducting computer monitoring or employee monitoring should ensure that the data collected directly satisfies the purpose of monitoring and that it clearly aligns with the need and objectives of the organization.[6]

A policy discussing the parameters of monitoring is in order to be able to ensure that the employees still have a reasonable expectation of privacy at work.[7] It is recommended to contain the following information:

- Purpose/s that computer monitoring seeks to fulfill;
- Circumstances of monitoring, including the time and place it may be conducted;
- The kinds of personal data that may be collected in the course of monitoring;
- Criteria for accessing monitoring records;
- Retention period of recordings or footages;
- Security measures pertaining to the storage, disclosure and disposal of recorded information;
- Authorized personnel who have access and control over the system in place; and
- Procedure on how employees may lodge complaint in case of violation of their rights, including the right to access their own personal data collected.[8]

Employers should keep in mind that although employees are within office premises and using company-issued equipment within office hours, they still are entitled to their right to privacy at work.

In the same way that the companies value the privacy rights of every customer, it should likewise respect the privacy of its own employees and enable them to exercise their rights. With the emergence of new technologies that provide employers with vast opportunities to monitor and track employees, unbridled checking can damage trust, disrupt professional relationships and disturb workplace peace and performance.[9] An effective policy and communication strategy must be implemented to maintain the balance between the business or operational objectives and the right to privacy.

---

[6] Privacy Commissioner for Personal Data, Hong Kong, supra note 3.

[7] Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work (08 June 2017), available at ec.europa.eu/newsroom/document.cfm?doc_id=45631 (last accessed Sept. 26, 2018).

[8] Supra note 5.

[9] Privacy Commissioner of New Zealand- Privacy at Work: A guide to the Privacy Act for employers and employees, accessed on 28 November 2018, available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-88

26 November 2018

[redacted]

Re: DENIAL OF REQUEST FOR DISCLOSURE OF THE PERSONAL DATA SHEET BY THE CITY OF SAN JUAN

Dear [redacted],

We write in response to your letter which sought to clarify whether the denial of your request for a certified true copy of the Personal Data Sheet (PDS) of your co-employee for record purposes and to prove that an act of perjury is committed, is in accordance with the Data Privacy Act of 2012 (DPA)[1] and NPC Advisory No. 2017-02 - Access to Personal Data Sheets of Government Personnel.[2]

We note that the decision of the San Juan City Human Resource Development Department to deny your request took into consideration the principles enunciated in the DPA and is consistent with the recommendations set by NPC Advisory No. 2017-02 on resolving a pending request for access to a PDS. This includes a statement from the City Human Resource Development Department of the City of San Juan, which you have attached, that a preliminary investigation is now being conducted by the Civil Service Commission (CSC) and docketed as Case No. D-1520001918 concerning your co-employee.

We wish to emphasize that access to or disclosure of the PDS of a particular government employee may be regulated despite its nature as a public record and/or public document. Each government agency may provide for certain rules or a set criteria against which a request for such document shall be assessed. A certified true copy of a Personal Data Sheet (PDS) of any government employee necessarily contains sensitive

[1] 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).
[2] National Privacy Commission, Access to Personal Data Sheets of Government Personnel, Circular No. 17-02 [NPC Circular 17-02] (April 3, 2017).

personal information such as civil status, blood type and other health information, GSIS, PAG-IBIG and PHILHEALTH No., information about the employee's family which may include information about minor children, among others. Thus, the disclosure of a certified Personal Data Sheet should be shown as necessary for the purpose of the requesting party, and such purpose must not be contrary to law, morals, and public policy.

We also note the statement in your letter that you have knowledge of the contents of the PDS of your co-employee as encoded in the Human Resource Information System (HRIS). In general, the HRIS of any agency should only be accessed by authorized personnel, and any access without clearance or authority may be considered unauthorized access or intentional breach depending on attendant circumstances.

This opinion is based solely on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning

ADVISORY OPINION
NO. 2018-90

28 November 2018

[redacted]

Re: DATA PRIVACY AND OFFICE-ISSUED MOBILE DEVICES

Dear [redacted],

We write in response to your inquiry regarding the use of office-issued mobile devices in relation to the Data Privacy Act of 20121 (DPA). In particular, you are asking whether the access of your employer to your personal iCloud account using an office-issued mobile device would be in violation of your rights to data privacy or constitute any of the offenses punishable under the DPA.

We understand that you were put under preventive suspension and as a result, your office-issued phone and laptop were confiscated. You were advised by your employer to remain logged in using your personal iCloud account in the office-issued phone. You then found out that selected conversations in the phone's messaging applications were shared in a meeting. Also, that Human Resource (HR) personnel were able to access your messages by reinstalling the messaging application using your personal iCloud account.

After this incident, you filed a case against your employer for constructive dismissal. Due to the severance of your contract and relationship with the company, you opted to log out of your iCloud account and removed access through the office-issued device. However, the HR has been requiring you to log back in in your personal iCloud and provide access to back up files even if you already resigned. Hence, the question of whether this may be considered a violation under the DPA.

[1] 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).

Reasonable expectation of privacy

The Supreme Court in **Ople v. Torres**[2] recognized the zones of privacy protected in our laws, based on the Civil Code provision which provides that every person shall respect the dignity, personality, privacy, and peace of mind of his neighbors and other persons. It also punishes as actionable torts several acts by a person of meddling and prying into the privacy of another.[3] Likewise, it recognized the privacy of communication and correspondence and holds a public officer or employee, or any private individual liable for damages for any violation of the rights and liberties of another person.[4]

The ruling in Ople v. Torres also expounded on the "reasonable expectation of privacy" test in ascertaining whether there is a violation of the right to privacy. This test determines whether a person has a reasonable or objective expectation of privacy and whether the expectation has been violated. The reasonableness of a person's expectation of privacy depends on a two-part test:

(1) whether by his conduct, the individual has exhibited an expectation of privacy; and
(2) whether this expectation is one that society recognizes as reasonable.

The factual circumstances of the case determine the reasonableness of the expectation. Similarly, customs, community norms, and practices may, therefore, limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy must then be determined on a case-to-case basis.[5]

Expectation of privacy in the employment context

It is noteworthy to mention that the reasonable expectation test was used at a time when the there were no laws on data protection and informational privacy.

Likewise, courts have generally held that employees have a decreased expectation of privacy with respect to work devices, email accounts, and internet surfing activities.[6] The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.

---

[2] GR No. 127685, July 23, 1998.
[3] Civil Code of the Philippines, Article 26.
[4] Id. Article 32.
[5] Id.
[6] See: Pollo v. David, G.R. No. 181881, (2011); O'Connor v. Ortega 480 U.S. 709 (1987).

Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.

By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA.[7] The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.

This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[8]

Considering this, companies should revisit policies on the use of electronic communication devices, taking into consideration the DPA, especially data privacy principles and data subjects' rights. This translates to clear and well-defined policies and practices as to the extent of monitoring, degree of intrusion, consequence to employees, and procedural guarantees against arbitrariness.

Expectation of privacy in personal iCloud account; unauthorized processing

The fact that an employer has the ownership of the electronic means does not rule out the right of employees to privacy of their communications, related location data and correspondence.[9] As such, employees have an expectation of privacy in their own personal iCloud accounts even if they are logged in using their office-issued mobile devices.

More recent jurisprudence in other jurisdictions also recognizes employee privacy in the workplace. In **Stengart v. Loving Care Agency Inc.**,[10] the New Jersey Supreme Court held that an employee has a reasonable expectation of privacy in her personal, web-based email correspondence using a company-owned laptop. The court recognized that though employers can enforce policies relating to computer use to protect the assets, reputation and productivity of a business, they

[7] Data Privacy Act of 2012, § 2.
[8] Id. § 11.
[9] Article 29 Working Party, Opinion 2/2017 on data processing at work (2017).
[10] 201 N.J. 300, 990 A.2d. 650 (2010)

nonetheless have no need or basis to read the specific contents of personal communications in order to enforce corporate policy.

In **Copland v. the United Kingdom**,[11] the European Court of Human Rights (ECtHR) held that monitoring of calls and email as well as personal internet usage in the workplace without the person's knowledge, amounted to an interference with her right to respect for her private life and correspondence. In another case[12] decided by the ECtHR, it was held that an employer's policy on monitoring communications in the workplace cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.

In your case, factual circumstances clearly show an expectation of privacy when you have taken precautionary steps to protect your privacy after being put in preventive suspension. Before surrendering the mobile device upon resignation, you opted to delete the messaging applications as well as the messages contained therein. Such expectation of privacy is reasonable considering that you have resigned from the company, and in light of the DPA.

The alleged use of your account to pry and investigate on other employees and the improper order from the management to not log out your account have put you on guard and secure your personal iCloud account.

Hence, the act of the HR employee of accessing your personal iCloud account without your consent may constitute violation of your privacy. Furthermore, such unauthorized access into may constitute unauthorized processing under the DPA. The elements of the offense are as follows:

1. the accused processed the information of the data subject;
2. that the information processed was personal information;
3. that the processing was done without the consent of the data subject, or without authority under this Act or any existing law.

An iCloud account is considered as personal information under the law.[13] As stated in your email, your personal iCloud was accessed without your express authorization and you were forced to log back in even after resignation. The act of the employer of accessing your iCloud account

[11] ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007.
[12] ECtHR, Barbulescu v. Romania [GC], No. 61496/08, 5 September 2017.
[13] Data Privacy Act of 2012, § 3 (g) *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.

without your knowledge and consent, and without authority under the law may be unauthorized processing of personal information.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

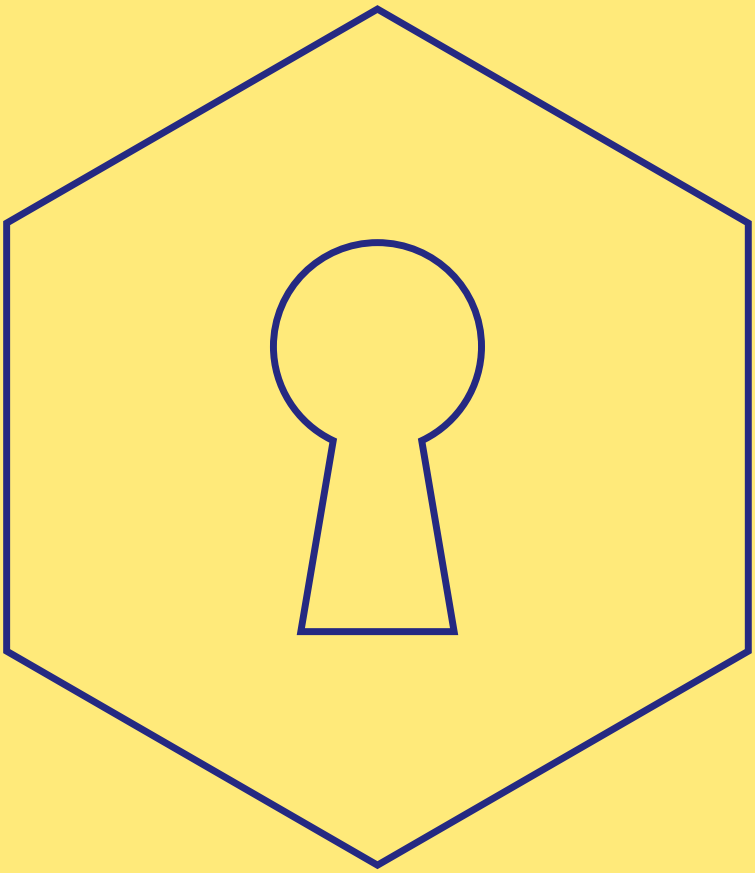
For your reference.

Very truly yours,

(Sgd) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman



NPC CASES & DECISIONS

NPC Case No. 18-058
WENDY'S RESTAURANT, INC. (PHILIPPINE REPRESENTATIVE OFFICE) DATA BREACH (2018)

NPC Case No. 17-043
JOLLIBEE FOODS CORPORATION

NPC Case No. 18-J-162
FACEBOOK FORCED LOGOUTn

NO. 18-058

RE: WENDY'S RESTAURANT, INC. (PHILIPPINE REPRESENTATIVE OFFICE) DATA BREACH (2018)

x----------x

ORDER

THIS ORDER is being issued under the power of this Commission to compel any entity to abide by its orders on a matter of data privacy, in relation to the data breach affecting Wenphil Corporation ("Wendy's") on 23 April 2018.

On 23 April 2018, yet unknown persons published online a database containing the Wendy's Philippine website in its entirety. This Commission obtained a copy of this database that same day.

On 26 April 2018, Wendy's Philippines notified this Commission that: (1) their website was infiltrated; (2) personal data has been exfiltrated; and (3) the database in the possession of the Commission is a true copy of the Wendy's online database from its Philippine website.

On an analysis of the information exfiltrated, it can be ascertained that the exposure of certain sensitive personal information or financial information within the database puts the affected data subjects in harm's way. There is a real risk of serious harm to the affected data subjects; the data is not merely incidental to the breach.

As such, the provisions on mandatory breach notification apply. Aside from notifying this Commission, these provisions also require adequate notificaion for data subjects, in a manner understandable to the data subjects.

On 2 May 2018, representatives from Wendy's appeared before this Commission to answer questions from the Complaints and Investigations Division on the facts and events surrounding the data breach. Unfortunately, the Wendy's Philippines were not able to provide any further details at the time.

At the same meeting, Wendy's acknowledged that it has yet to inform the affected data subject of the note, scope, and extent of the breach, notwithstanding the clear mandate of NPC Circular No. 16-03 on breach notifications, and the contents thereof. These requirements were brought to the attention of the representatives.

The Wendy's representatives also admitted that earlier attempts at implementing security measures were thwarted when these ICT officers resigned before any of the measures were implemented. They also admitted that most JCT security for the website was left to the discretion of their webhost.

To facilitate the investigation, the Complaints and Investigations Division also required Wendy's to provide further documentary evidence on earlier attempts at implementing stronger data protection measures.

WHEREFORE, PREMISES CONSIDERED, this Commission hereby **ORDERS** Wenphil Corporation to:

1. **NOTIFY** all affected data subjects with exposed sensitive personal information or information that can be used to enable identity fraud, pursuant to the requirements contained within NPC Circular No. 16-03 within 72 hours from the issuance of this Order;

2. **EXPLAIN** to this Commission why further action should not be taken against Wenphil Corporation for their failure to notify the affected data subjects within the proper period required in NPC Circular No. 16-03.

3. **PROVIDE** a copy of Server Logs, Network Logs, and Traffic Logs of the https://wend\'s.com.ph website prior to the breach;

4. **SUBMIT** the updated version of the applicable Privacy Policy in force at the time of the data breach, an update of the internal investigation conducted, and the policy on transaction procedures, and any and all prior recommendations for information security measures that were not implemented.

5. **CONDUCT** a new Privacy Impact Assessment, taking into account the vulnerabilities exposed in this latest data breach.

SO ORDERED.

2 May 2018, Pasay City, Metro Manila.

For the Commission:

(Sgd.) FRANCIS EUSTON R. ACERO
Division Chief
Complaints and Investigations Division

NPC CASES & DECISIONS
NO. 17-043

RE: JOLLIBEE FOODS CORPORATION

x----------x

ORDER

THIS ORDER is being issued under the power of this Commission to compel any entity to abide by its orders on a matter of data privacy, in relation to a data breach report submitted by Jollibee Foods Corporation (Jollibee or JFC) last 12 December 2017.

In the Breach Notification, JFC Group DPO J'Mabelard M. Gustilo informed the Commission that on 8 December 2017, persons unknown to the JFC Group appeared to have been able to gain access to the customer database of the delivery website for Jollibee.

In the course of the investigation, the Complaints and Investigation Division (CID) identified the breach to be a result of a proof-of-concept initiated by a marketing PR team representative of Jollibee, who made representations to a domestic cybersecurity firm.

On 21 December 2017, the CID invited said firm to a meeting wherein one of its members narrated that he, while conducting vulnerability testing for another client, noticed a security gap in the jollibeedelivery.com website. While their group was able to exploit the vulnerabilities, their firm insisted that they did not scrape or exfiltrate any data, because they merely demonstrated their ability to access the data in Jollibee's database if they so desired.

Shortly after the breach, Gustilo decided to handle corrective measures internally and through its third party IT security providers. Gustilo nevertheless clarified that the JFC Group treated the cybersecurity firm responsible for the breach as an uncontracted entity or stranger who had no authority to infiltrate their IT infrastructure.

In a later meeting, Gustilo admitted to the CID that the database protection was not up to date, and some data, including personal information, were unencrypted. Although CID noted some improvements

in protecting data privacy on the part of the JFC Group after the suspected breach, more consistent and effective efforts are needed to protect the data. As DPO, Gustilo acknowledged difficulty in effecting the needed data protection and security measures for various reasons, such as budgetary constraints, low prioritization or outright disinterest within the organization.

Following these meetings, on 20 February 2018, the CID began conducting its own vulnerability assessment of Jollibee's website and found that it remains vulnerable to unauthorized access. Such vulnerabilities may allow malefactors with little to moderate technical knowledge and skill to access personal information of Jollibee patrons through its website.

Considering that smaller systems with more robust security measures have been exposed, there is a very high risk that approximately 18 million people currently on the database will be exposed to harm.

Considering, further, that these vulnerabilities were made known to Jollibee for quite some time, and that their online properties remain vulnerable, urgent action is necessary to protect the personal data of those using the JFC Group delivery service.

WHEREFORE, PREMISES CONSIDERED, this Commission, through its Legal and Enforcement Office, hereby **ORDERS** Jollibee Foods Corporation to:

1. **SUSPEND** forthwith the operations of jollibeedelivery.com and all other data processing open to the public through the internet and restrict external access to their networks, for an indefinite time until the site's identified vulnerabilities are addressed, as validated by a duly certified penetration testing methodology.
2. **SUBMIT** a security plan to be implemented in rehabilitating said system to ensure the integrity and retention of the database and its content within ten (10) calendar days upon receipt hereof.
3. **EMPLOY** Privacy by Design in the reengineering of JFC Group data infrastructure.

4. **CONDUCT** a new Privacy Impact Assessment, considering the vulnerabilities exposed in the Commission's penetration tests and in subsequent penetration tests ordered in the next preceding section.
5. **FILE** a monthly Progress Report on this matter until the issues raised in this Order are resolved.

Given in the Meeting dated 4 May 2018 with Jollibee Foods Corporation at this Commission's offices at the Philippine International Convention Center.

SO ORDERED.

4 May 2018, Pasay City, Metro Manila.

For the Commission:

(Sgd.) FRANCIS EUSTON R. ACERO Division Chief
Complaints and Investigations Division

Approved by:

(Sgd.) GILBERT V. SANTOS
OIC-Director IV
Legal and Enforcement Office

NPC CASES & DECISIONS
NO. 18-J-162

In Re: Facebook Forced Logout

x----------x

ORDER

THIS ORDER is being issued under the power of this Commission to compel or petition any entity to abide by its order or take action on a matter affecting data privacy,[1] in relation to an ongoing investigation on Facebook Inc. ("Facebook") concerning the exploitation of the "View As" feature to extract a user's access tokens without their consent.

On 25 September 2018, Facebook discovered that there was an unexpected increase in traffic on the use of the "View As" feature. Based on its declaration, it is believed that this was introduced into Facebook's code on 12 July 2017. However, Facebook believes that the attack may have only commenced on 14 September 2018, the date when the spike in traffic commenced.

Three (3) days after the vulnerability was discovered by Facebook, 28 September 2018, the vulnerability was then allegedly fixed and Facebook notified all its users via an in-app update message supposedly on the same date.[2] The Commission was then informed through e-mail at 12:40 a.m. of the next succeeding day, 29 September 2018.

On 2 October, in a conference call with Facebook officials and this Commission, Facebook, through counsel, informed this Commission that individual notification was not deemed ripe as the conditions for individual notification under Circular No. 16-03 were not yet met. At the same meeting, Facebook expressed a commitment to abide by Philippine data privacy laws.

On 13 October, Facebook informed the National Privacy Commission that of the 30 million people with stolen access tokens, they now believe that a total of 755,973 Philippine-based Facebook user accounts may have been compromised that forced Facebook to log out users from their accounts last September 28.

[1] Sec. 7(d) Republic Act No. 10173, Data Privacy Act of 2012.
[2] Facebook Letter, Subject: Incident Update from Facebook, Inc., 13 October 2018

Facebook categorizes the affected users into three distinct groups, or "buckets" based on the personal information the perpetrator may have accessed.

The first bucket involves an estimated 387,322 Philippine-based user accounts whose basic profile information may have been compromised. Basic profile information consists of a user's registered full name, email address, and phone number (if one was so associated with the account). The second bucket affects around 361,227 Philippine-based user accounts. In addition to the basic profile information potentially obtained as with the first group of users, the perpetrator may have also obtained:

a. Username,
b. First name used on the profile,
c. Last name used on the profile,
d. Name (nickname as set by the user on the profile (if any)),
e. Email address (primary email address associated with the account),
f. Phone (confirmed mobile phone numbers associated with account),
g. Gender (as set by the user on the profile),
h. Locale (language as picked by the user),
i. Relationship status (as set by the user on the profile),
j. Religion (as described by the user on the profile),
k. Hometown (as set by the user on the profile),
l. Location (current city, as set by the user on the profile),
m. Birthday (as set by the user on the profile),
n. Devices (that are used by the user to access Facebook - fields include 'os' (e.g., iOS) and hardware (e.g., iPhone),
o. Educational background (as set by the user on the profile),
p. Work history (as set by the user on the profile),
q. Website (list of URLs entered by the user into the website field on the profile),
r. Verified status information (this is a flag for whether Facebook has a strong indication that the user is who they say they are),
s. List of most recent places where the user has checked in (these locations are determined by the places named in the posts, such as a landmark or restaurant, not location data from a device),
t. Recent search queries on Facebook, and
u. Up to the top 500 accounts that the user follows.

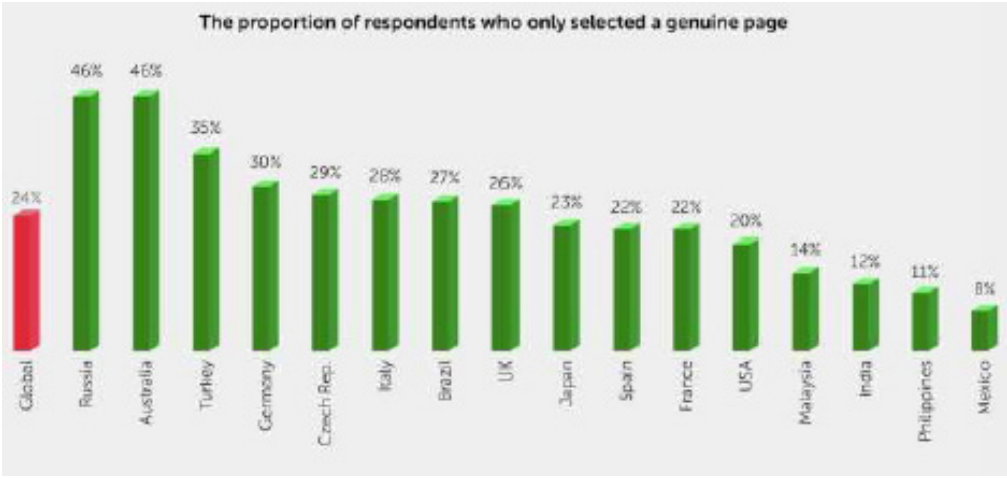
The third bucket involves 7,424 Philippine-based users. In addition to the data potentially obtained in relation to the first two groups of users,

further information that may have been exposed include the posts on their timeline, their list of friends, groups they are members of, and the names of recent Messenger conversations.

From the tenor of the document, we now understand that the breach exposed the personal information of persons with accounts that fall under any of the three buckets, to different degrees. Be that as it may, Facebook contends in its letter dated 13 October 2018 that there is no material risk of more extensive harm occurring.

This Commission does not agree; the risk of serious harm to Filipino data subjects is more than palpable. The conditions for individual notification are present.

As Facebook itself notes, the main potential impact for affected users will be an increased likelihood of getting targeted for professional "spam" operations and "phishing" attacks. However, the risk and vulnerability of Filipinos to spam and phishing are regarded as one of the highest in the world. According to the Are You Cyber Savvy Report from Kaspersky Lab, approximately 9 out of 10 Filipinos are susceptible to phishing attacks.[3]



The level of awareness for spam, phishing and identity theft in the Philippines is not the same as those of the United States and the other developed nations; considerations of risk must always consider the cultural milieu in which the risk is appreciated. For instance, this Commission takes notice that identity verification systems throughout the Philippines are quite weak.

[3] https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234157/Cyber_savvy_quiz_report.pdf (last accessed 18 October 2018).

As a milieu, the increase in risk for phishing and/or identity theft is self-evident for those persons who were exposed through the unauthorized use of the access tokens.

The Commission therefore deems it necessary that Facebook contemplate this cultural gap when notifying the affected data subjects. Facebook should modify its approach and provide a more conducive method that enables affected Filipino data subjects to better grasp the risks they face.

The potential deleterious effects of a breach should not be diluted in the notification to the data subjects. Data breach notifications for data subjects are for their benefit; we must provide as much information as possible to assist the affected data subjects to brace for its impact.

The manner and method of this notification is clearly defined under Section 18 of NPC Circular 16-03.

Facebook is hereby mandated to submit a more comprehensive Data Breach Notification Report and inform the data subjects in compliance with the provisions of NPC Circular No. 16-03 – Personal Data Breach Management.

Due to the nature and exposure of the Filipino data subjects, Facebook must also provide for identity theft insurance or credit monitoring service for free to affected Filipino data subjects; or, in the alternative, establish a dedicated helpdesk/help center for Filipino data subjects who may be adversely affected by this incident, to provide assistance in identity restoration and other related matters.

WHEREFORE, PREMISES CONSIDERED, this Commission, hereby **ORDERS** Facebook to:

1. **SUBMIT** a more comprehensive Data Breach Notification Report to this Commission following rules laid down in NPC Circular No. 16-03;
2. **NOTIFY** the affected data subjects through an appropriate Data Breach Notification following rules laid down in NPC Circular No.
16- 03;
3. **PROVIDE** identity theft and phishing insurance for affected Filipino data subjects, or in the alternative, ESTABLISH a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning Facebook, located in the Philippines and with a local number, within six (6) months from receipt of this Order;

4. **IMPLEMENT** a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness on identity theft and phishing; and
5. **PROVIDE** evidence of compliance with the foregoing.

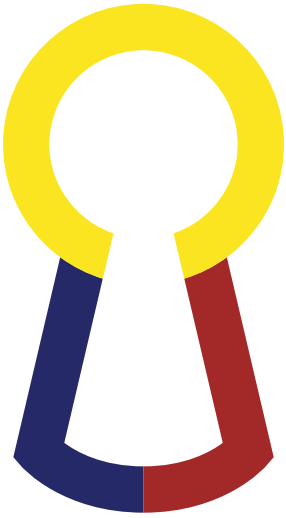
Given thru electronic mail and by hand, 17 October 2018.

SO ORDERED.

October 17, 2018, Pasay City, Metro Manila.

For the Commission:

(Signed)
(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner



NATIONAL
PRIVACY
COMMISSION

5th Floor, Delegation Building
Philippine International Convention Center
PICC Complex, Roxas Boulevard, Manila, 1307

privacy.gov.ph
info@privacy.gov.ph
privacy.gov.ph
PrivacyPH
privacygovph
234-22-28