Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-051

5 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 personal 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.

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;

[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).

(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?*

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)?*

[3] Republic Act No. 10173, § 12 and 13.
[4] See: Revised Rules on Evidence, Rule 130, §24.
[5] Republic Act No. 10173, § 3(k).

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 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:

(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;

---

[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).
[8] *Id*., §18 (b).
[9] *Id*., §18 (c).
[10] Republic Act No. 10173, §16.

(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.

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]

11. *"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.

[11] NPC Advisory Opinion No. 2017-64
[12] GR No. L-75885, May 27, 1987.
[13] Republic Act No. 10173, §16(c).
[14] *Id.*, §16(c).

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 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]

12. *"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

---

[15] *Id*., § 3(c).
[16] *Id*., § 3(j).
[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).

that the personal 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.

13. *"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.

14. *"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]

---

[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.*
[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).

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