Republic of the Philippines
NATIONAL PRIVACY COMMISSION

# PRIVACY POLICY OFFICE
# ADVISORY OPINION NO. 2019-034[1]

02 September 2019

[redacted]

**Re: CONSENT AND ITS WITHDRAWAL FOR EMPLOYMENT PURPOSES**

Dear [redacted],

We write in response to your query which sought to clarify matters regarding the Data Privacy Act of 2012 (DPA),[2] specifically on the consent of job applicants and existing company employees. You sought our opinion on the following scenarios where employers require consent forms:

- as a pre-employment requirement, enumerating the various purposes for the same, i.e. candidate screening, salary offer calculation, as well the submission of police clearance, etc.;

- as an employment requirement where all the required information and purposes of data processing are enumerated including, but not limited to: issuance of a company ID, determination of health conditions and fitness to work, verification of employment history, facilitate processing of ATM payroll, assess, update and provide employee entitlements, approve and verify claims with respect to benefits granted by the company, improve and maintain effective employee administration, manage work activities and personnel, communication, maintenance of employment records, employee data in accounting and tax system, team building activities, imposition of disciplinary actions, potential legal claims, and HR safety requirements and fire safety instructions; and

- allowing the company to conduct extensive background investigation during the probationary period of employment.

We understand that job applicants who refuse to sign the consent form would not be considered for employment, and those under probationary employment will not be considered for permanent employment.

Relating to the given scenarios, you specifically asked the following:

[1] Tags: consent; freely given; specific; employees; employment; transparency; privacy notice; lawful processing.
[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).

- What are the criteria applied by the Commission in assessing if the consent of the data subject was "freely given" and "specific"? Is the consent given by the data subjects under the scenarios considered freely given and specific?

- If the consent of the data subjects obtained under the foregoing scenarios fails to satisfy the requirements of the DPA and the Implementing Rules and Regulations (IRR), would the employer be required to divide its purposes for data processing into (a) lawful processing purposes (which do not require consent for processing) and (b) other specific purposes, and obtain the data subject's consent only for those other specific purposes?

- To what extent should an employer apply the requirements under the General Data Protection Regulation (GDPR)? If not applicable, please clarify the differences, if any, between the concept of consent under the DPA and consent under GDPR.

- If consent given by the data subject is not considered as freely given and specific, is it sufficient that they are given an opportunity to withdraw consent?

- Will the withdrawal of consent affect the lawfulness of the processing based on consent before its withdrawal? Should the processing be discontinued immediately or is it sufficient that it be discontinued as soon as practicable, particularly when immediate stoppage is not possible?

- Assuming that a data subject withdraws consent, but the processing may still fall under other instances of lawful processing under Sections 12 and 13 of the DPA, can a personal information controller (PIC) continue to process the personal data?

- Are PICs prohibited from using the terms "consent" or "agree" in the privacy notice or consent form addressed to data subjects with information required under Section 16(b) of the DPA if the PICs know from the very beginning that even if the data subject withdraws consent, they will still process the personal data in accordance with some other lawful purpose under the DPA?

*Criteria applied in assessing if consent was "freely given", "specific" and "informed"*

Under Section 3(b) of the DPA, 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. Thus, the definition of consent indicates three requirements, namely: freely given, specific, and informed indication of will.

In order to assess whether a data subject's consent was "freely given," "specific" and "informed," the DPA requires adherence to the principle of transparency, requiring PICs to inform data subjects 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 PIC, his or her rights as a data subject, and how these can be exercised.[3] Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[4] Thus, validity of consent will depend on the data subject's comprehension of the disclosures made by the PIC. It is only with sufficient comprehension that a data subject will be able to exercise real choice in providing consent.

[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (2016).
[4] *Id.*

Further, we note the pertinent discussions in Opinion 15/2011[5] on the definition of consent of the Article 29 Data Protection Working Party of the European Commission, specifically on whether the same may be considered as freely given in the context of an employer-employee relationship, to wit:

> "Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free. xxx xxx xxx
>
> An example of the above is provided by the case where the data subject is under the influence of the data controller, such as an employment relationship. In this example, although not necessarily always, the data subject can be in a situation of dependence on the data controller - due to the nature of the relationship or to special circumstances - and might fear that he could be treated differently if he does not consent to the data processing. xxx xxx xxx
>
> Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment. If, once consent is withdrawn, the data processing continues based on another legal ground, doubts could be raised as to the original use of consent as the initial legal ground: if the processing could have taken place from the beginning using this other ground, presenting the individual with a situation where he is asked to consent to the processing could be considered as misleading or inherently unfair."

In addition, Opinion 2/2017[6] on data processing at work reinforces the above:

> "WP29 has previously outlined in Opinion 8/2001 that where an employer has to process personal data of his/her employees it is misleading to start with the supposition that the processing can be legitimised through the employees' consent. In cases where an employer says they require consent and there is a real or potential relevant prejudice that arises from the employee not consenting (which can be highly probable in the employment context, especially when it concerns the employer tracking the behaviour of the employee over time), then the consent is not valid since it is not and cannot be freely given. Thus, for the majority of the cases of employees' data processing, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required.
>
> Moreover, even in cases where consent could be said to constitute a valid legal basis of such a processing (i.e. if it can be undoubtedly concluded that the consent is freely given), it needs to be a specific and informed indication of the employee's wishes..."

For the requirement that consent be specific, Article 29 Data Protection Working Party opined[7] that "specific consent is therefore intrinsically linked to the fact that consent must be informed. There is a requirement of granularity of the consent with regard to the different elements that constitute the data processing: it cannot be held to cover 'all the legitimate purposes' followed by

---

[5] European Commission, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, pages 12-13, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed: 27 May 2019).

[6] European Commission, Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 8 June 2017, pages 6-7, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (last accessed: 27 May 2019).

[7] European Commission, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, page 17, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed: 27 May 2019).

the data controller. Consent should refer to the processing that is reasonable and necessary in relation to the purpose."[8]

Granularity of consent necessarily dictates that in the case of multiple purposes, different purposes must be unbundled, and separate consent must be obtained for each purpose. As we stated in our Advisory Opinion 2018-063, "[c]onsent 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."[9] PICs may determine which purposes may be grouped together or separated based on what is reasonable and necessary and obtain separate consent for each accordingly.

Furthermore, consent must be intelligible. It should refer clearly and precisely to the scope and the consequences of the data processing. Consent cannot apply to an open-ended set of processing activities. This means that the context in which consent applies is limited.[10] Considering such, a PIC may ask for more than one consent for every purpose it may have. By doing so, a data subject is given more preference as to how their information will be processed rather than obtaining an "all or nothing" consent which cannot be considered freely given.

In addition, consent shall be evidenced by written, electronic or recorded means. Any of the required formats may be adopted by a PIC as the NPC does not maintain any preference. 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 and not necessarily just a positive act showing a data subject has opted in.[11]

*Necessity of requiring employer to divide the purposes for data processing; other lawful criteria for processing aside from consent*

The processing of personal information is permitted under the DPA when at least one of the conditions provided under Section 12 is present. As to sensitive personal information, its processing is prohibited except when there exists any of the cases enumerated under Section 13 of the DPA.

As enunciated in NPC Advisory Opinion No. 2017-050:

> A Personal Information Controller (PIC), such as your employer, can also process personal information when it is necessary and is related to the fulfillment of a contract with the data subject, such as a contract for employment. This would include computation and payment of salaries and other benefits, determination of career movements, facilitation of work-related requirements, and outsourcing of human resource management functions.
>
> Another instance is when the processing of personal information is necessary for compliance with a legal obligation to which the personal information controller is subject and when processing is provided for by existing laws and regulations. This would include compliance with statutory and regulatory requirements of national government agencies, to which your employer is subject to.

[8] *Id.*
[9] National Privacy Commission, NPC Advisory Opinion No. 2018-063 (October 23, 2018) citing 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.
[10] *Id.*
[11] National Privacy Commission, NPC Advisory Opinion No. 2017-007 (Jan. 9, 2017).

> In fact, consent in the abovementioned instances may not even be required by the DPA, since the processing would fall under another criteria for lawful processing.
>
> Note also the special cases where the DPA is not applicable on certain specified information, i.e. information necessary in order to carry out the functions of public authority. Hence, the processing of your personal data as an employee in compliance with labor and tax laws are actually outside of the scope of the DPA, to the minimum extent necessary to achieve the specific purpose, function, or activity of the public authority. [12]

From the foregoing, it is clear that consent is not the only basis for an employer to lawfully process personal data. In relation to processing with multiple purposes, PICs should be cognizant of all processing activities by conducting a Privacy Impact Assessment (PIA) to come up with a data inventory, description of the processing operations, assessment of the necessity and proportionality of the processing, and assessment of the risks, among others. Through the PIA, the PIC will be able to determine the most appropriate lawful criteria for such processing, which in the case of employment-related processing need not necessarily be consent.

*Consent under the DPA vis-à-vis consent under GDPR*

Consent was defined in the European Union (EU) General Data Protection Regulation (GDPR) in the following manner:

> 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[13]

On the other hand, Section 3(b) of the DPA specifically defines consent thus:

> 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.

The above definitions are essentially the similar. While it is true that the Commission often examines EU opinions, laws, and jurisprudence for analogous cases in interpreting the provisions of the DPA, as the latter was highly influenced by the 1995 EU Data Protection Directive, the predecessor of the GDPR, we reiterate the statement in NPC Advisory Opinion 2017-009[14] that the Philippines is not a member of the European Union and therefore not bound by its policies (1995 EU Directive and its successor, GDPR). Neither is the DPA nor its IRR meant to directly enforce the said EU regulations.

Thus, for processing that is under the scope of the DPA, the requirements relating to consent as provided therein shall prevail. Should an employer be likewise subject to the GDPR, such employer shall adhere to both the DPA and the GDPR.

*Data subject's rights; withdrawal of consent*

[12] National Privacy Commission, NPC Advisory Opinion No. 2017-050 (Aug. 29, 2017).
[13] 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, Article 4 (11) (2016).
[14] National Privacy Commission, NPC Advisory Opinion No. 2017-009 (Jan. 16, 2017).

When consent is the lawful basis for processing, data subjects have the right to object and withhold consent to the processing of his or her personal data, unless the processing is under the following conditions:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
3. The information is being collected and processed as a result of a legal obligation.[15]

Where consent is the proper basis for processing, and the same is withdrawn by the data subject, the same should not affect the lawfulness of the processing before the withdrawal of such consent. However, the same is not true in cases where the consent given does not meet the standards set by the DPA. In such cases, other lawful criteria must serve as basis for the processing of information because merely giving a data subject an opportunity to withdraw an irregularly-given consent will not cure such defect. Consent that is not freely given and specific will be tantamount to an implied consent which cannot be sanctioned by the Commission.

In all instances therefore, PICs are reminded to have policies and processes in place to document the consent obtained, its subsequent withdrawal, as well as the procedure on discontinuing the processing of personal data.

*Privacy notices; consent forms; right to be informed*

Further in your inquiry, clarification is being sought whether the use of the words "consent" or "agree" in privacy notices or consent forms is prohibited in cases where PICs know from the beginning that even if the data subjects withdraw their consent, personal data will still be processed.

We reiterate NPC Advisory Opinion No. 2018-013[16] which discussed at length the difference between privacy notices and consent:

> "…A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.
>
> 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. xxx
>
> 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."

Hence, using such words in a privacy notice is not advisable as the same should be used in a consent form instead.

[15]Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 34 (b) (2016).
[16] National Privacy Commission, NPC Advisory Opinion No. 2018-013 (April 18, 2018).

As mentioned above, PICs should be able to determine the most appropriate criteria for processing personal and sensitive personal information. PICs should not get consent if the same is not appropriate and necessary in relation to the purpose of processing, and especially in instances where the PIC is already aware that such processing will still continue despite the withdrawal of consent.

This opinion is based 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.) RAYMUND ENRIQUEZ LIBORO**
Privacy Commissioner and Chairman