28 October 2019

ADVISORY OPINION

Reference No. DPO 19-48

FOR : [redacted]

[redacted]

SUBJECT : **Consent form for Personnel**

Dear [redacted] and [redacted]:

We received your referral of the attached [redacted] mandating that all UP personnel should sign the attached "Data Privacy Consent Form".

Advisory Opinion

For the following reasons, the "Data Privacy Consent Form" is unnecessary and may cause issues:

1. UP does not need the consent of its employees:
    a. Processing of personal information related to an employment contract (or similar contracts) does not require consent;
    b. Processing of personal information based on a legal mandate (or to comply with laws) does not require consent;
    c. It is not common practice for employers to request for consent of its employees.

2. Asking for consent will give employees the peculiar authority to withhold or withdraw UP's right to process their personal information. UP will have a problematic situation wherein it will have to treat differently those who did not sign the consent form from those who did.

3. The consent form does not comply with legal requirements:
    a. Consent should be for *specific* information processing activities and "bundled" consent using "blanket statements" is prohibited;

b. Consent should be “time-bound”.

4. The UP System’s Privacy Notice for Personnel (referred to in the consent form) disrupts the observance of the pre-existing UP Diliman Privacy Notice for Staff.
    a. Having two documents with the same subject matter brings confusing implementation. UP Diliman cannot suddenly shift its initiatives because it already has been building its privacy resilience based on its own pre-existing policies;
    b. Only the DPO which UP Diliman registered with the NPC may render issuances for UP Diliman;
    c. Experience with the NDA that was required from employees reveal that a good number of UP Diliman employees are averse to being required to sign documents that may limit their freedoms.

To avoid legal, operational and relational issues with its thousands of employees, it is suggested that UP Diliman does not require signing of the Data Subject Consent Form.

Discussion

Statement in the Consent Form

Below is the statement in the Data Privacy Consent Form:

> “This is to certify that:
>
> I have read the University of the Philippines System Privacy Notice for Personnel.
>
> I understand that for the UP System to carry out its functions as the National University pursuant to the UP Charter, exercise its right to academic freedom under the 1987 Constitution, pursue its legitimate interests as allowed by the Data Privacy Act of 2012, and comply with legal obligations, lawful issuances or orders of other public authorities, as well as contractual obligations to me, UP must necessarily process my personal and sensitive personal information.
>
> I grant my consent to and recognize the authority of the UP System (including its constituent universities and the offices thereunder) to process my personal and sensitive personal information pursuant to the abovementioned privacy notice and applicable laws.”

Consent is not always required before personal information can be processed. As the National Privacy Commission (NPC) states: *“The law provides for instances when processing of personal and sensitive personal information, which may include collection, use, disclosure,*

and outsourcing thereof, is permitted under the law. Consent of the data subject to the processing is only one of the instances."[1]

UP does not need the consent of its employees –

Processing of personal information related to an employment contract does not require consent

UP has a contract with its employees, whether they be probationary, regular, contractual or UP contractual employees. Consent of employees is not required when the processing of personal information is necessary and related to the fulfillment of a contract to an employment contract. The Data Privacy Act of 2012 states:

> "SEC. 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:
>
> *x x x*
>
> (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;"[2]

Since the actions of UP as an employer is related to an employment contract, consent is not necessary.

Not only is consent unnecessary for processing in relation to an employment contract, consent is also unwarranted when the processing is for the legitimate interest of an employer. As the NPC explained in its advisory opinion:

> "In the case of an employer, as a personal information controller (PIC), the processing of personal information of its employees is allowed when it is necessary and in relation to the fulfillment of an employer-employee contract.
> **Processing may also be done for purposes of the legitimate interests pursued by the employer.** Lastly, the processing is allowed when it is necessary for compliance with a legal obligation to which the employer is subject such as when required under labor laws and regulations. In the abovementioned cases, **consent of the employees to the processing need not be obtained.** However, with regard to processing of sensitive personal information, consent of employees is required unless processing falls under any of the other instances provided in Section 13."[3]

As long as the processing of personal information is necessary for the *legitimate interests* of UP, consent is not required. This is well-founded in the law which states:

---

[1] NPC Advisory Opinion No. 2017-50.
[2] Data Privacy Act of 2012, Section 12(b).
[3] NPC Advisory Opinion No. 2017-51.

> "SEC. 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:
>
> *x x x*
>
> (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."[4]

The NPC illustrated the breadth of employer actions that can be done without consent in another advisory opinion:

> "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.**
>
> In fact, consent in the abovementioned instances may not even 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."[5]

If an objective of the consent form is to cover UP's other other activities which are not related to its employer-employee relationship with its personnel, then the consent form is not the solution because its scope only covers the data subjects' role as UP's "personnel". As discussed hereafter, if consent would be required for a purpose not related to employment, the consent form should be specific to such purpose.

[4] Data Privacy Act of 2012, Section 12(f).
[5] NPC Advisory Opinion No. 2017-50.

Processing of personal information based on a legal mandate (or to comply with laws) does not require consent

UP has the legal mandate to operate as a "university for the Philippine Islands"[6] with "general powers of administration"[7]. UP's "general powers of administration" includes its power to administer matters related to employment.

Personal information may be processed if necessary for compliance with a legal obligation, the Data Privacy Act of 2012 states:

> "SEC. 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:
>
> *x x x*
>
> (c) The processing is necessary for **compliance with a legal obligation** to which the personal information controller is subject;"

Sensitive personal information may be processed if provided for by law, the same Act further states:

> "SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> *x x x*
>
> (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;"

The primary laws that establish UP's legal mandates (Act No. 1870 and Republic Act No. 9500) qualify as "law" which allows for processing of sensitive personal information; as the NPC clarified:

> "Law, in the context of the DPA, is understood in its generic sense. It would include statutes enacted by the legislature, presidential issuances such as executive orders, administrative orders, rules and regulations…"[8]

NPC Advisory Opinion No. 2018-007 further states:

[6] Act No. 1870.
[7] *Idem,* Section 6.
[8] NPC Advisory Opinion No. 2017-28.

> "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."

Hence, information provided to UP either for UP's processing or for submission to other government instrumentalities such as DOLE and BIR do not require consent. The NPC stated:

> "As to personal data needed for government requirements, this falls under 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 the employees' personal data in compliance with labor and tax laws, among others, 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."[9]

It is not common practice that employers request for consent of employees

Beyond theories, there is also wisdom in being mindful of industry practices. It is not common for employers to request for the consent of their employees. Perhaps there can be something learned from the fact that thousands of data protection officers do not request for the consent of their organizations' employees.

Asking for consent will result in a situation wherein UP will have to treat differently those who gave consent and those who did not

Consent should not be coerced but instead "freely given"[10]. It may be withdrawn.[11] Requesting for employee consent will corner UP in a situation wherein it would give those did not provide consent (or withdrew their consent) a different treatment from those who provided consent. To date, a good number of employees continue to refuse to sign the Non-Disclosure Agreement (NDA) required by UP. It is advisable that a similar conundrum be avoided by not creating and giving a new power to employees: the power to withhold or withdraw UP's right to process their personal information.

Even experts on GDPR, the draft of which was the part-basis of the Data Protection Act of 2012,

> "Indeed, the European guidance notes that **for the majority of data processing at work, the lawful basis "cannot and should not be the consent of employees"**. Furthermore, GDPR makes clear that it is not permissible to rely on consent if a

[9] NPC Advisory Opinion No. 2017-51.
[10] Data Privacy Act of 2012, Section 3(b).
[11] *Idem,* Section 19(a)(1).

contract is made conditional on the consent, notwithstanding that the consent is not strictly necessary for the performance of the contract.

For these reasons, **we would recommend that consent is not relied on by an employer as a basis for processing employee personal data.** Trying to rely on consent against these clear restrictions will only therefore cause greater difficulties for employers in practice. For example, it will give an employee strong grounds to delay or even prevent an investigation, grievance or disciplinary process if based on monitoring that the employee had invalidly consented to."[12]

The consent form does not comply with legal requirements –

Consent should be for specific information processing activities and "bundled" consent using "blanket statements" is prohibited

The Data Privacy Consent Form does not contemplate specific acts of processing of personal information but instead broad classes of processing. This is prohibited since consent should be specific to the purpose of the intended processing; the law states:

> "c. '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."[13]

This is in line with the principle of providing specific information to the data subject:

> "2. The data subject must be provided **specific information** regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing."

In an advisory opinion, the NPC stated that *"a 'bundled' consent will generally not suffice as the data subject is not empowered to make a true choice"*[14]. In another advisory opinion, "blanket statements" of a consent form invalidated the requirements of having *"specific and informed indication of will"*.[15]

[12] Dunne, Bryan; O'Sullivan, Tina; O'Brien Finín, "How to navigate employee consent under GDPR", SiliconRepublic, May 4, 2018, https://www.siliconrepublic.com/enterprise/consent-gdpr-employees, accessed October 27, 2019.
[13] Data Privacy Act of 2012, Section 3(c).
[14] NPC Advisory Opinion No. 2018-063.
[15] NPC Advisory Opinion No. 2017-42.

In a [redacted] guidance of the [redacted], consent is held inappropriate for an employer processing employee data:

> "When is consent inappropriate?
>
> It follows that if for any reason you cannot offer people a genuine choice over how you use their data, consent will not be the appropriate basis for processing. This may be the case if, for example:
>
> *x x x*
>
> - you are in a position of power over the individual – for example, if you are a public authority or an employer processing employee data."[16]

The Data Subject Consent Form has a single paragraph comprised of a single sentence stating what the consent is for. In a similar previous incident, the NPC struck down a single-sentenced paragraph consent for not giving the data subject genuine choice, the NPC stated:

> "**All of the above are enumerated and combined in a single paragraph.** As mentioned, consent, where required, should be specific. **Having an 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."[17]

Consent should be "time-bound"

"When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose."[18] The consent form provided is has no period and is not time-bound. In an advisory opinion, the NPC stated that *"consent cannot be overly broad and perpetual, for this would undermine the very concept of consent".*[19]

The UP System's Privacy Notice for Personnel disrupts the observance of the prior UP Diliman Privacy Notice for Staff

The Data Privacy Consent Form refers to its related document, the UP Privacy Notice for Personnel. It is worth clarifying that there can be no consent to a notice. The NPC elucidated that: *"Being a mere notice, it is emphasized that the privacy notice is not equivalent to consent."*[20]

---

[16] Information Commissioner's Office (United Kingdom), "Consultation: GDPR consent guidance", March 31, 2017, https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf, accessed October 27, 2019.
[17] NPC Advisory Opinion No. 2018-063.
[18] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 19(a)(1).
[19] NPC Advisory Opinion No. 2017-23.
[20] NPC Advisory Opinion No. 2018-013.

There is a pre-existing UP Diliman Privacy Notice for Staff which is applicable to UP Diliman Staff, including Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, and retirees. There is also a pre-existing UP Diliman Privacy Policy for Applicant Students, Faculty and Staff. Both can be found in UP Diliman's privacy portal at upd.edu.ph/privacy. The actions, decisions, advice and training provided by the UP Diliman Data Protection Team are based on these policies, among others. Suddenly releasing a new overlapping document without any consultation with any of the Constituent Universities (CUs) will have the disruptive and confusing result of having two policies implemented for the same subject matter. UP Diliman cannot suddenly shift its initiatives because it already has been building its privacy resilience based on its own pre-existing policies.

Under Office of the Chancellor Administrative Order No. MLT 19-073, the UP Diliman Data Protection Officer has *"autonomy and independence"*[21] in the responsibility to *"Promulgate policies rules and guidelines related to data privacy, information security, data governance, and related frameworks"*[22]. This is in line with NPC Circular No. 2017-01 which requires *"To strengthen the autonomy of the DPO or COP and ensure the independent nature of his or her role"*.

Only one Data Protection Officer (DPO) is registered with the National Privacy Commission (NPC) for each Personal Information Controller (PIC). UP Diliman is a separate PIC from the UP System because it controls a different set of personal information as an autonomous CU. It is the registered DPO of a PIC which has the authority and jurisdiction over the data protection of his organization. This is the reason why it is the registered DPO of a PIC has the *"accountability"* to comply with laws and regulations.[23]

Experience with the NDA that was previously required from employees reveal that a good number of UP Diliman employees are averse to being required to sign documents that may limit their freedoms. If employees are asked to sign the consent form, there will be a cobweb of employee classes – there will be employees that signed both the NDA and the Data Privacy Consent Form, those who did not, and the combinations in between. There will be unequal treatment of thousands of employees depending on which documents they did or did not sign.

It is suggested to not ask employees to sign the consent form as it is unnecessary and will only cause legal, compliance, logistical and relational issues with employees.

[21] Office of the Chancellor Administrative Order No. MLT 19-073, Section V.
[22] *Idem,* Section III(a).
[23] NPC Circular No. 2017-01.

Conclusion

The Data Subject Consent Form is unnecessary since UP is acting in relation to an employment contract, in pursuance of its legal mandate, and in compliance with laws. Asking for consent will just give employees the bizarre authority to withhold or withdraw UP's right to process their personal information. In addition, the consent form does not comply with legal requirements: it bundled consent using blanket statements and it is not time-bound. There is already a pre-existing UP Diliman Privacy Policy for Staff. Having another overlapping policy will confuse implementation and disrupt pre-existing initiatives. To avoid legal, operational and relational issues with its employees, it is suggested that UP Diliman does not ask employees to sign the consent form.

Please feel free to reach out for clarifications or further concerns.

Yours,

(Sgd.) Elson B. Manahan
Data Protection Officer
University of the Philippines Diliman