Republic of the Philippines
NATIONAL PRIVACY COMMISSION

# PRIVACY POLICY OFFICE
# ADVISORY OPINION NO. 2018-041

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.

[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).

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.

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

---

[2] Data Privacy Act of 2012, §3(i).
[3] *Id.*, §3(l)(3).
[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.*

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 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.