Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
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. 10173 (2012).
[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173.

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