# PRIVACY POLICY OFFICE
# ADVISORY OPINION NO. 2017-001

5 January 2017

[redacted]

**Re: REGISTRATION OF PROCESSING SYSTEM FOR ONLINE BUSINESSES; DELETION OF DATA PROVIDED UNDER SECTION 34(E) OF THE IMPLEMENTING RULES AND REGULATIONS (IRR) OF THE DATA PRIVACY ACT (DPA); AND CLARIFICATION ON SECTION 19(E)(2) OF THE IRR IN RELATION TO DELETION OF PERSONAL INFORMATION**

Dear [redacted],

This pertains to your queries received by the National Privacy Commision (NPC) on 7 November 2016, via email. Specifically, your questions pertain to the following:

a. "requirements, process and possible timeline for processing of online businesses";
b. any regulations issued by the NPC regarding the retention and deletion of personal data. In particular, you asked "whether the deletion of data as stated in Section 34.e of the Data Privacy Act (sic) pertains to deletion from online site/platform only or should the deletion extend to the systems backup as well"; and
c. "clarification or further explanation on the application of Section 19.e.2 of the Data Privacy Act (sic)" in relation to the deletion of personal information.

*Requirements, Process and Possible Timeline for Processing of Online Businesses*

The DPA and its IRR require the registration of the personal data processing systems of personal information controllers (PICs) or personal information processors (PIPs).[1] However, PICs or PIPs that employ fewer than two hundred fifty (250) persons are not required to register, unless the following conditions are present:

- the processing they carry out are likely to pose a risk to the rights and freedoms of data subjects; or
- the processing is not occasional; or
- the processing includes sensitive personal information of at least one thousand (1,000) individuals.

[1] *see*: Republic Act No. 10173, § 24, and IRR of RA 10173, § 47.

The foregoing rules do not distinguish as to the type of business or industry of a PIC or PIP in determining if the latter is obliged to comply. In view thereof, online businesses are deemed subject to the same set of regulations.

To date, the primary policy reference for the registration of personal data processing systems is Section 47 of the IRR. It lists down the registration information that need to be forwarded by the concerned PICs and PIPs to the Commission. One of the information required is the name of the compliance or data protection officer and his or her contact details.

As regards the period for compliance, Section 67 of the IRR is instructive:

> "Personal information controllers and Personal information processors shall register with the Commission their data processing systems or automated processing operations, subject to notification, within one (1) year after the effectivity of these Rules… xx x xx
>
> For a period of one (1) year from the effectivity of these Rules, a personal information controller or personal information processor may apply for an extension of the period within which to comply with the issuances of the Commission. The Commission may grant such request for good cause shown." (underscoring supplied)

*Regulations Regarding the Retention and Deletion of Personal Data*

As per Section 11(e) of the DPA, personal information shall be "retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law". Section 19(d) of the IRR echoes this policy and provides:

> "d. Personal Data shall not be retained longer than necessary.
>
> 1. Retention of personal data shall only for as long as necessary:
>    (a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
>    (b) for the establishment, exercise or defense of legal claims; or
>    (c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
>
> 2. Retention of personal data shall be allowed in cases provided by law.
> 3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects."

Meanwhile, Section 16(e) of the DPA grants every data subject the right to "suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected". In the IRR, Section 34(e) states:

"e. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:
   (a) The personal data is incomplete, outdated, false, or unlawfully obtained;
   (b) The personal data is being used for purpose not authorized by the data subject;
   (c) The personal data is no longer necessary for the purposes for which they were collected;
   (d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
   (e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
   (f) The processing is unlawful;
   (g) The personal information controller or personal information processor violated the rights of the data subject.
2. The personal information controller may notify third parties who have previously received such processed personal information."

Based on the foregoing provisions of the law and its IRR, it is apparent that no distinction or qualification is made as to where (i.e., online site/platform vs. systems backup) the deletion (or conversely, retention) shall apply or refer to. Accordingly, when the law does not distinguish, we must not distinguish ("*Ubi lex non distinguit nec nos distinguire debemus*").[2]

The claim forwarded that "portion of the backup cannot be deleted without jeopardizing the system backup" is unsubstantiated, and requires proof. As per the basic legal maxim, he who alleges must prove his case.[3] In this regard, it has to be adequately proven that deletion of a portion of a backup system will negatively impact such system. Only then can the Commission entertain alternative proposals for compliance with the provisions of the law.

*Clarification re: application of Section 19.e.2 of the IRR in relation to the deletion of personal information*

Section 19(e)(2) of the IRR provides:

"Section 19. General principles in collection, processing and retention. The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data: xxx xxx xxx

e. Any authorized further processing shall have adequate safeguards.
xxx xxx xxx

[2] *Amores v. House of Representatives*, G.R. No. 189600, 29 June 2010.
[3] *Lim v. Equitable PCI Bank*, G.R. No. 183918, 15 January 2014.

> 2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose."

The provision pertains to the authorized further processing and the retention of personal data that have already been transformed into an aggregated or anonymized state. What were previously considered personal data have been rendered anonymous, such that the data may no longer be associated or traced back to a specific person or individual.

In relation to deletion, we believe that a data subject no longer has any right to erasure, as provided under Section 34(e) of the IRR, if the data concerned has already been aggregated or anonymized.

Since anonymized data refers to data or information that may not be traced back to a particular person or individual, they do not constitute personal data, as defined by the IRR. Accordingly, given that a data subject may only assert his or her rights under the DPA relative to his or her personal data, he or she may not invoke or exercise such rights in relation to other types of data, including anonymized data.

For your reference.

Sincerely,

**JAMAEL A. JACOB**
Director, Privacy Policy Office

Approved:

**IVY D. PATDU**
Deputy Privacy Commissioner,
Policy and Planning