



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-021**

14 June 2017



Re: SCOPE OF THE DATA PRIVACY ACT OF 2012

Dear 

This pertains to your query received by the National Privacy Commission (NPC) on 12 May 2017, via email, which sought to clarify the following matters regarding Republic Act No. 10173¹, also known as the Data Privacy Act of 2012 (DPA):

1. Whether the cooperatives registered under the Cooperative Development Authority (CDA) are covered by the DPA;
2. If indeed the cooperatives are covered by the law, determine the following:
 - a. Obligations of cooperatives
 - b. Reportorial requirements to be submitted to the NPC
 - c. Compliance period for such requirements
 - d. Penalties for non-compliance; and
3. Where cooperatives may course through or communicate other concerns regarding data privacy.

Scope

The DPA applies to “any natural and juridical person involved in the personal information² processing including those personal information controllers³ and processors⁴ who, although

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” (15 August 2012).

² *Id.*, §3(g) *Personal Information* refers to 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.

³ *Id.*, §3(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. This term excludes: (1) A person or organization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes or use personal information in connection with the individual’s personal, family or household affairs.

not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.”⁵

Upon examination of the nature of information handled by the CDA and cooperatives, it is clear that cooperatives may be considered as personal information controllers (PICs) who collect, hold, process and use personal information of its members.

Republic Act No. 6939⁶ created the CDA to formulate plans and programs on cooperative development, including the development and conduct of management and training programs to assist members and ensure the viability and growth of cooperatives.⁷ Most importantly, it is in-charge of the registration of all cooperatives, federations and unions.⁸

Pursuant to this function, cooperatives are mandated to register as a cooperative and provide documents to the CDA, including financial and membership details.⁹ As you have also mentioned in your email, cooperatives process personal data of members, particularly with regard to the application and processing of their individual loans. Thus, both the CDA and cooperatives under it are involved in the processing of personal and sensitive personal information and are thereby obliged to adhere with the provisions of the DPA.

We understand that cooperatives are also considered as submitting entities¹⁰ under the Credit Information System Act (CISA) and are required to submit credit information to the Credit Information Corporation (CIC), given that cooperatives are classified as “credit facilities” that provide loans, credit lines or other forms of financial accommodation.¹¹

Due to this, they are directed to submit credit data of its members in order for the CIC to perform its duty to establish a comprehensive and centralized credit information system for the entire Philippines.¹²

It is imperative to note that cooperatives process personal information of its members and employees as part of its regular operations. The credit data or loan information mentioned is just a segment personal information collected and stored by cooperatives.

Nevertheless, for a more comprehensive response to your inquiry, it must be stated that the information submitted to the CIC by cooperatives is listed among those considered by the DPA as a special case.

⁴ *Id.*, §3(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

⁵ *Id.*, §4.

⁶ AN ACT CREATING THE COOPERATIVE DEVELOPMENT AUTHORITY TO PROMOTE THE VIABILITY AND GROWTH OF COOPERATIVES AS INSTRUMENTS OF EQUITY, SOCIAL JUSTICE AND ECONOMIC DEVELOPMENT, DEFINING ITS POWERS, FUNCTIONS AND RESPONSIBILITIES, RATIONALIZING GOVERNMENT POLICIES AND AGENCIES WITH COOPERATIVE FUNCTIONS, SUPPORTING COOPERATIVE DEVELOPMENT, TRANSFERRING THE REGISTRATION AND REGULATION FUNCTIONS OF EXISTING GOVERNMENT AGENCIES ON COOPERATIVES AS SUCH AND CONSOLIDATING THE SAME WITH THE AUTHORITY, APPROPRIATING FUNDS THEREFOR, AND FOR OTHER PURPOSES (10 March 1990).

⁷ *Id.*, §3(a&b).

⁸ *Id.*, §3(e).

⁹ CDA Memorandum Circular 2015-01 on the Revised Guidelines Governing the Registration of Cooperatives.

¹⁰ RA No. 9510, AN ACT ESTABLISHING THE CREDIT INFORMATION SYSTEM AND FOR OTHER PURPOSES, “Credit Information System Act” (31 October 2008), §3(q)

¹¹*Id.*, §3(f).

¹² *Id.*, §2.

Section 4 of the law and Section 5 of the Implementing Rules and Regulations (IRR) exempt specific types or classes of information from its scope - in particular, paragraph (e) of the latter states:

“Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned: xxx

- e. *Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or **Bangko Sentral ng Pilipinas, and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws; xxx***

Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.” (Emphasis supplied).

From the provision above, it is evident that the processing of credit data or financial information required to be submitted to the CIC, in compliance with its mandate under the CISA, is exempt from the coverage of the DPA, but only to the minimum extent necessary to achieve the specific purpose, function, or activity, and the cooperatives are still bound to implement the necessary security measures to protect personal information it processes, and adhere to the other provisions of the DPA.

Cooperatives as Personal Information Controllers or Processors are mandated to comply with the directives provide by the DPA, its IRR and other NPC issuances

Cooperatives are obliged to comply with the provisions of the DPA, its IRR and other NPC issuances that are relevant to their sector and to the nature of information that they are processing.

Chief among these obligations is the adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality. PICs and personal information processors (PIPs) are also mandated to uphold the rights of the data subjects.

Another requirement is the need to appoint a data protection officer (DPO). Pursuant to Section 21(b) of the DPA and Section 50(b) of the IRR, PICs shall designate an individual or individuals who are accountable for the organization’s compliance with this Act. This is further elucidated under NPC Advisory No. 2017-01 dated 14 March 2017 stating that all natural or juridical persons, or any other body in the government of private sector engaged in the processing of personal data within and outside of the Philippines. The DPO will

ensure that the entity complies with the provisions of the law and other relevant rules and regulations on data privacy and security.

Cooperatives as PICs (or PIPs) are likewise required to implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.¹³

We also wish to emphasize the NPC's circulars on data sharing agreements involving the government (NPC Circular No. 2016-02) and personal data breach management (NPC Circular No. 2016-03). The first circular requires the review of all existing data sharing arrangements and/or actual contracts, joint issuances, or any similar documents, and make the necessary revisions thereto, execution of a data sharing agreement where applicable, and the immediate termination of the sharing of personal data in instances where the arrangement is not for the purpose of performing a public function or providing a public service, and the second pertains to the policies required to be implemented, reportorial requirements, and notifications relating to personal data breaches.

Reportorial requirements to be submitted by cooperatives to the NPC

Registration requirement

Section 47 of the IRR of the DPA provides for the registration of personal data processing systems. This provision states that if a personal information controller or personal information processor employs at least two hundred fifty (250) persons, registration is automatically required.

When the personnel employed are fewer than two hundred fifty (250), registration is not required, unless the any of the following circumstances is present:

1. The processing it carries out is likely to pose a risk to the rights and freedoms of the data subjects;
2. The processing is not occasional; or
3. The processing includes sensitive personal information of at least one thousand (1,000) individuals.

In case any of the circumstances enumerated above are present, the cooperative is then required to register its data processing system.

The NPC will be implementing the registration process in two phases: Phase I requires the submission of a notarized registration form containing details on the PIC, head of the organization, and the DPO, and Phase II is the registration of the data processing systems to be done online.

As the NPC is still in the process of optimizing its website for the Phase II endeavor, for purposes of the September 2017 deadline, only Phase I will be strictly required. The public is advised to visit the website of the NPC for any updates and announcements on the implementation and deadline for Phase II.

¹³ DPA, §20

Data Breach Notification

A PIC is required to notify the NPC and the affected data subjects “within seventy-two (72) hours upon knowledge of, or when there is reasonable belief that a personal data breach has occurred”.¹⁴ The report may be submitted in a written or electronic format¹⁵ containing the required contents of the notification stated in Sections 20(f) and 39 of the DPA and the IRR, respectively.

NPC Circular 16-03¹⁶ comprehensively discusses the framework for personal data breach management and the procedures for personal data breach notification, as well as the requirement for the submission of the annual report of all personal data breaches and security incidents.

Notification of Automated Decision-Making

A personal information controller “carrying out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes shall notify the Commission when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject”.¹⁷

As of the moment, the NPC does not require any format for the notification, as long as it contains the contents enumerated in Section 48 of the IRR.

Penalties imposable for violations and non-compliance with the provisions of the DPA, its IRR and other NPC issuances

The law and the IRR do not provide for penalties for non-compliance with the appointment of the DPO, registration of data processing systems, notification of automated decision-making, submission of annual reports, among others.

However, in case of the occurrence of a personal data breach, the filing of a complaint by a data subject, or an audit of the Commission, compliance with such requirements shall be considered by the NPC in evaluating the situation and its determination of liability under the penal provisions¹⁸, if any.

Furthermore, the DPA provides for the violations and penalties under the law, which includes: (a) unauthorized processing of personal information and sensitive personal information; (b) accessing personal information and sensitive personal information due to negligence; (c) improper disposal of personal information and sensitive personal information; (d) processing of personal information and sensitive personal information for unauthorized purposes; (e) unauthorized access or intentional breach; (f) concealment of security breaches involving sensitive personal information; (g) malicious disclosure; (h) unauthorized disclosure; or (i) combination or series of acts.

¹⁴ IRR of the DPA, §38(a).

¹⁵ IRR of the DPA, §41(a).

¹⁶ Available at www.privacy.gov.ph

¹⁷ IRR of the DPA, §48.

¹⁸ See DPA, §25-33

A minimum fine of one hundred thousand pesos (PhP 100,000.00) to a maximum of five million pesos (PhP 5,000,000.00), *and* a minimum imprisonment period of six (6) months to a maximum of seven (7) years shall be imposed on the offender depending on the violation.

When personal information of at least one hundred (100) persons is harmed, affected or involved as a result of the action/s, the maximum penalty in the scale of penalties shall be imposed.¹⁹

Lastly, it is important to note Section 34 of the DPA, to wit:

“SECTION 34. Extent of Liability. – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.”

Other concerns

Questions and clarifications may be e-mailed to info@privacy.gov.ph. Complaints may be submitted to complaints@privacy.gov.ph. You may also visit NPC’s website, www.privacy.gov.ph for other services.

For your reference.

Sincerely,

RAYMUND E. LIBORO
Privacy Commissioner and Chairman

¹⁹ DPA, §35.