



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-014¹**

05 March 2019



**Re: PROPOSED BANGKO SENTRAL NG PILIPINAS AND
DEPARTMENT OF INTERIOR AND LOCAL GOVERNMENT
JOINT MEMORANDUM CIRCULAR IN THE ISSUANCE OF
BUSINESS LICENSE/PERMIT FOR PAWNSHOPS AND
MONEY SERVICE BUSINESSES**

Dear 

We write in response to your request for an advisory opinion on the proposed Joint Memorandum Circular (JMC) which will be issued by the Bangko Sentral ng Pilipinas (BSP) and the Department of Interior and Local Government (DILG).

Specifically, Clause 6.2 thereof provides that each city or municipality shall submit to the BSP a duly certified report, containing the names of Pawnshops (PSs) and Money Service Businesses (MSBs):

1. That were issued new business licenses/permits;
2. Renewed their business licenses/permits;
3. Failed to renew business licenses/permits; and
4. That cancelled/revoked/retired their business permits.

BSP shall then determine and communicate with the pertinent LGUs which PSs and MSBs are:

1. Have BSP registration and with LGU business permit engaged in business activities which are consistent or inconsistent with those stated in the BSP registration;
2. With BSP registration but without LGU business permit;
3. Without BSP registration but with LGU business permit - includes those with and without pending application for registration with BSP; and
4. Without BSP registration and LGU business permit.

We understand that the following issues arose in the course of finalizing the JMC:

¹ Tags: Scope, personal information, special cases,
5th Floor Delegation Building, PICC Complex, Roxas Boulevard, Pasay City, Metro Manila
URL: <https://privacy.gov.ph> Email Add: info@privacy.gov.ph

1. Whether or not the information shared under Clause 6.2 of the proposed JMC is covered by the Data Privacy Act of 2012² (DPA);
2. Assuming that the information to be shared is considered personal information, whether or not data sharing between DILG and BSP is allowed under the DPA; and
3. In the affirmative, whether BSP and DILG are required to enter into a separate data sharing agreement or the proposed JMC is sufficient in order to share the information.

Scope of the DPA; personal information; special cases

The information of juridical entities is outside of the scope of the DPA, as the DPA applies solely to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.

While the information of PSs and MSBs operating as sole proprietorships or partnerships may be considered as personal information as the identity of the owner/s can be reasonably and directly ascertained by the BSP and the DILG, their personal information may fall under the exclusions under Section 4(e) and/or 4(f) of the DPA, to wit:

“SECTION 4. *Scope.* — xxx xxx xxx

This Act does not apply to the following: xxx xxx xxx

- (e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act. No 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
- (f) Information necessary for banks and other financial institutions under the jurisdiction of the independent central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; xxx.”

For Section 4(e), the exclusion particularly pertains to information necessary in carrying out the functions of a public authority, which includes processing for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.

However, the exclusions above are not absolute. The exclusion of the information specified in Section 4 of the DPA is only to the minimum extent necessary to achieve the specific purpose, function, or activity. Thus, the use of the information claimed to be outside the scope of the DPA:

1. Must be necessary in order to carry out the functions of public authority; and
2. The processing of personal data is for the performance of a constitutional or statutory

² 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).

mandate.³

Similarly, for Section 4(f), the exclusion applies to information necessary for banks and other financial institutions under the jurisdiction of the BSP to comply with the following:

1. Republic Act No. 9510 - Credit Information System Act (CISA);
2. Republic Act No. 9160 - Anti-Money Laundering Act; and
3. Other applicable laws.

Given this, the personal and sensitive personal information (collectively, personal data) enumerated in Section 4 may be lawfully processed by a PIC, even without meeting the conditions under Sections 12 and 13 of the DPA, but the processing shall be limited to that necessary to achieve the specific purpose, function, or activity. The PIC is still required, however, to implement measures to secure and protect the personal data.⁴

Thus, only the information required to be processed pursuant to the said function are not covered by the law, while the PICs are still covered by the DPA. The BSP and the DILG are mandated under the DPA to adhere to the data privacy principles of transparency, legitimate purpose, and proportionality, implement appropriate security measures for personal data protection, and ensure that data subjects are able to exercise their rights as provided for by law.

Data sharing

Data sharing shall be allowed when it is expressly authorized by law. Further, Section 20 (d) of the IRR recognizes the data sharing between and among government agencies for the purpose of a public function or provision of a public service. The same section provides that the sharing arrangement shall be covered by a data sharing agreement (DSA), and that:

1. All parties to the agreement shall comply with the DPA, its IRR, and issuances of the NPC, including putting in place adequate safeguards for data privacy and security; and
2. The DSA shall be subject to review of the NPC, on its own initiative or upon complaint of a data subject.

The proposed sharing between the BSP and the LGUs is allowed under the DPA and its IRR as the same is necessary in relation to the specific mandates of these government agencies.

There is legitimate purpose in the sharing of the personal data, as this will aid in the determination of PSs and MSBs' compliance with the pertinent BSP and LGU registrations.

The information to be shared, as described in the JMC, are the minimum information required to determine compliance with existing laws and regulations, and hence, proportional and not excessive in relation to the purpose of the sharing arrangement.

On transparency and upholding the rights of the data subjects to be informed, it is advisable that owners of the PSs and MSBs be informed about the sharing arrangement. This may be done through a privacy notice.

³ See: National Privacy Commission, NPC Advisory Opinions No. 2018-002 (Jan. 15, 2018), 2018-014 (May 9, 2018), and 2018-060 (Aug. 30, 2018).

⁴ See: National Privacy Commission, NPC Advisory Opinion No. 2018-060 (Aug. 30, 2018).

Data sharing agreement in a Joint Memorandum Circular

NPC Circular No. 16-02 was enacted to govern data sharing involving government agencies.

As defined in the circular, a data sharing agreement is a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties.⁵ With regard to the contents of a data sharing agreement, Section 6 enumerates the terms and conditions that must be complied with and must be included in the agreement.

The proposed JMC, specifically Clauses 6.2, 6.3 and 7.0 thereof, as currently drafted, may not be sufficient for the purposes of complying with the Circular. Clauses 6.2 and 6.3 merely indicate the overview of the operational details of the sharing or transfer of personal data and Clause 7.0 provides for the confidentiality requirement. There are several other items which must be included, to wit:

ELEMENTS	DETAILS / REMARKS
A. Term or duration of the agreement	<p>The JMC should specify the term or duration of the sharing arrangement, which may be renewed on the ground that the purpose or purposes of such agreement continues to exist, provided that in no case such term or any subsequent extension exceed five (5) years, without prejudice to entering into a new agreement.</p> <p>A provision on the exact term or duration of the agreement should be added which should not exceed more than five (5) years subject to renewal.</p>
B. General description of the security measures, including the policy for retention or disposal of records	<p>There is a need to provide a general description of the physical, technical, and organizational security measures that will ensure the protection of the personal data.</p> <p>Likewise, any policies on retention or disposal of records should be reflected in the JMC.</p>
C. Where online access to personal data will be provided	<p>The following items must be indicated</p> <ol style="list-style-type: none"> 1. justification for online access; 2. parties granted online access; 3. types of personal data accessible online; 4. estimated frequency and volume of the proposed access; 5. program and middleware; and 6. encryption method
D. The personal information controller responsible for addressing: (1) information requests; and	Not indicated

⁵ National Privacy Commission, Data Sharing Agreements Involving Government Agencies, Circular No. 16-02 [NPC Circular 16-02] § 3 (E) (October 10, 2016).

(2) complaints filed by data subjects and/or is being investigated by the NPC	
E. Method for the secure return, destruction, or disposal of the shared data (including the timeline)	Not indicated
F. The designated data protection officer or compliance officer	Not indicated

The NPC, the DPA, its IRR, and issuances of the Commission do not limit the agreement of the parties provided that the agreement does not contravene the letter and intent of the law. The Commission fully subscribes to the fundamental legal tenet ascribing a presumption of regularity in the performance of functions by government agencies.

Finally, please note that a data sharing agreement does not require prior approval from the NPC.

This opinion is rendered based on the 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