Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-52

11 September 2017

[redacted]

Dear [redacted],

This has reference to your letter dated 18 August 2017 and received by the National Privacy Commission (the Commission) on 22 August 2017, on the request for clarification on whether the Anti-Money Laundering Council (AMLC) may be exempted from the requirements of NPC Circular No. 16-02 - Data Sharing Agreements Involving Government Agencies.

We understand that AMLC is a financial intelligence unit tasked to implement the Anti-Money Laundering Act (AMLA). It has the following functions:[1]

1. to require and receive covered or suspicious transaction reports from covered persons;

2. to issue orders addressed to the appropriate Supervising Authority or the covered person to determine the true identity of the owner of any monetary instrument or property subject of a covered or suspicious transaction report, or request for assistance from a foreign State, or believed by the AMLC, on the basis of substantial evidence, to be, in whole or in part, wherever located, representing, involving, or related to, directly or indirectly, in any manner or by any means, the proceeds of any unlawful activity;

3. to institute civil forfeiture proceedings and all other remedial proceedings through the Office of the Solicitor General;

4. to file complaints with the Department of Justice or the Office of the Ombudsman for the prosecution of money laundering offenses and other violations under the AMLA;

[1] 2016 Revised Implementing Rules and Regulations, Republic Act No. 9160, as amended, Rule 7(B)

5. to investigate suspicious transactions and covered transactions deemed suspicious after investigation by the AMLC, money laundering activities and other violations of the AMLA;

6. to file with the Court of Appeals, ex parte, through the Office of the Solicitor General:

    a. a petition for the freezing of any monetary instrument or property that is in any way related to an unlawful activity; or
    b. an application for authority to inquire into or examine any particular deposit or investment, including related accounts, with any banking institution or non-bank financial institution;

7. to formulate and implement such measures as may be necessary and justified under the AMLA to counteract money laundering;

8. to receive and take action in respect of any request from foreign states for assistance in their own anti-money laundering operations as provided in the AMLA;

9. to develop educational programs, including awareness campaign on the pernicious effects, the methods and techniques used, and the viable means of preventing money laundering and the effective ways of prosecuting and punishing offenders;

10. to enlist the assistance of any branch, department, bureau, office, agency or instrumentality of the government, including government-owned and -controlled corporations, in undertaking any and all anti-money laundering operations, which may include the use of its personnel, facilities and resources for the more resolute prevention, detection and investigation of money laundering offenses and prosecution of offenders;

11. to impose administrative sanctions for the violation of laws, rules, regulations, orders, and resolutions issued pursuant thereto; and

12. to require the Land Registration Authority and all its Registries of Deeds to submit to the AMLC, reports on all real estate transactions involving an amount in excess of Five Hundred Thousand Pesos (Php500,000.00) within fifteen (15) days from the date of registration of the transaction, in a form to be prescribed by the AMLC. The AMLC may also require the Land Registration Authority and all its Registries of Deeds to submit copies of relevant documents of all real estate transactions.

Indeed, the AMLC is exempt from obtaining consent from data subjects when processing personal data pursuant to its statutorily mandated functions. This applies when obtaining information provided by banks and other financial institutions necessary to comply with the Anti-Money Laundering Act. It must be noted that the information is limited to that authorized by R.A. No. 9160, as amended, requiring reporting of covered and suspicious transactions by covered persons.

The AMLC may request for "Know-Your-Customer" documents from covered persons only to the extent necessary for the purposes specified under Section 7(2) of Republic Act No. 9160, as amended. This means that unless the documents requested pertain to a covered or suspicious transaction report, or to a request of assistance from a foreign State related to proceeds of an unlawful activity as supported by substantial evidence, the documents may not be subject of a valid request.

We understand that the AMLC shares the collected information with law enforcement agencies (LEA) and other government agencies "to serve as leads in their respective investigations and only for intelligence purposes." It is important to document the legal basis for this sharing, including what information will be shared. Data sharing between government agencies for the purpose of a public function or provision of a public service is not prohibited but shall be covered a data sharing agreement, unless the sharing of information is specifically provided by the Constitution or by law. For instance, R.A. No. 9160, as amended, specifically provides that covered persons shall report to AMLC all covered and suspicious transactions. Because a law specifically requires this reporting, a data sharing agreement is not necessary. Thus, unless similar provisions exist for sharing of information with law enforcement agencies and other government agencies, the sharing of collected information should be covered by a Data Sharing Agreement.

Data Sharing between government agencies for purpose of a public function or provision of a public service is not prohibited provided that the function or service is consistent with and necessarily required under the general mandate of the agencies concerned. It is in these cases, when there is no specific and explicit provision for processing of personal data, that a data sharing agreement is necessary. The agreement will document the basis of the processing, and ensure that parties involved in the data sharing will comply with the Data Privacy Act, and remain mindful of the rights of data subject, and the corresponding obligations to protect personal data. Information to be shared should only be to the minimum extent necessary to achieve the specific and legitimate purpose, function, or activity, and should not be used to circumvent the requirements of Article III, Sections 1, 2 and 3 of the 1987 Constitution. It may be necessary to note that the wide latitude to collect information given to the AMLC under the law is for purpose of ensuring that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity. Any processing outside this purpose should be justified by a Constitutional or statutory mandate.

AMLC has existing memoranda of agreement (MOA) or memoranda of understanding (MOU) on these information sharing arrangements.

In NPC Circular No. 16-02, there are several requirements for data sharing and data sharing agreements. In view of the general request for exemption and the fact that the Commission was not provided a copy of a sample MOA or MOU, we shall instead discuss each item required under the said circular and provide our remarks thereto based on the limited information provided to the Commission:

	Requirement	Remarks
Consent	The personal information controller charged with the collection of personal data directly from the data subject, on its own or through a personal information processor, shall obtain the consent of the data subject prior to collection and processing, except where such consent is not required for the lawful processing of personal data, as provided by law.	The collection of personal data from the covered institutions and the sharing thereof to law enforcement and other government agencies, pursuant to the provisions of the AMLA, its IRR and issuances of the AMLC, are exempt for the consent requirement.
Data Privacy Principles	Data sharing shall adhere to the data privacy principles laid down in the Act, the IRR, this Circular, and all applicable issuances of the Commission.	All personal information controllers (PICs) and personal information processors (PIPs) are required to adhere to these principles.
Contents of a Data Sharing Agreement	A. It shall specify, with due particularity, the purpose or purposes of the data sharing agreement, including the public function or public service the performance or provision of which the agreement is meant to facilitate: *Provided*, that if the purpose includes the grant of online access to personal data, or if access is open to the public or private entities, these shall also be clearly specified in the agreement.	The MOA/MOU should have provision/s on this item.
	B. It shall identify all personal information controllers that are party to the agreement, and for every party, specify: 1. the type of personal data to be shared under the agreement; 2. any personal information processor that will have access to or process the personal data, including the types of processing it shall be allowed to perform;	The MOA/MOU should have provision/s on this item.

	Requirement	Remarks
	3. how the party may use or process the personal data, including, but not limited to, online access; 4. the remedies available to a data subject, in case the processing of personal data violates his or her rights, and how these may be exercised; 5. the designated data protection officer or compliance officer.	
	C. It shall specify the term or duration of the agreement, which may be renewed on the ground that the purpose or purposes of such agreement continues to exist: Provided, that in no case shall such term or any subsequent extensions thereof exceed five (5) years, without prejudice to entering into a new data sharing agreement.	We understand that the current MOAs/MOUs do not have fixed terms, and the AMLC is concerned that providing for a five-year term may hamper its functions as there may be administrative matters to be resolved every time AMLC would have to renew the MOAs or MOUs. The reason for the need to enter into a new data sharing agreement is to take into account possible changes in law and regulation, technological advancements and other circumstances which may require a review of terms and conditions of the MOA or MOU to ensure that personal data is protected according to best practices.
	D. It shall contain an overview of the operational details of the sharing or transfer of personal data under the agreement. Such overview must adequately explain to a data subject and the Commission the need for the agreement, and the procedure that the parties intend to observe in implementing the same.	The MOA/MOU should have provision/s on this item, insofar as to explain to the Commission the details of the sharing.
	E. It shall include a general description of the security measures that will ensure the protection of the personal data of data subjects, including the policy for retention or disposal of records.	The MOA/MOU should have provision/s on this item.
	F. It shall state how a copy of the agreement may be accessed by a data subject: *Provided*, that the government agency may redact or prevent the disclosure of any detail or information that could endanger its computer network or system, or expose to harm the integrity, availability or confidentiality of	Due to the nature of the sharing arrangement, we believe that data subjects' request for access to the MOAs/MOUs should be evaluated on a case to case basis, taking into consideration pending investigations, etc.

	Requirement	Remarks
	personal data under its control or custody. Such information may include the program, middleware and encryption method in use, as provided in the next succeeding paragraph.	The MOAs/MOUs do not, as a general rule, contain any confidential information but merely provides the obligations of each party to the agreement. To the extent that an investigation will not be affected, the rights of data subjects should be upheld.
	G. If a personal information controller shall grant online access to personal data under its control or custody, it shall specify the following information: 1. Justification for allowing online access; 2. Parties that shall be granted online access; 3. Types of personal data that shall be made accessible online; 4. Estimated frequency and volume of the proposed access; and 5. Program, middleware and encryption method that will be used.	The MOA/MOU should have provision/s on this item.
	H. It shall specify the personal information controller responsible for addressing any information request, or any complaint filed by a data subject and/or any investigation by the Commission: *Provided*, that the Commission shall make the final determination as to which personal information controller is liable for any breach or violation of the Act, its IRR, or any applicable issuance of the Commission.	The MOA/MOU should have provision/s on this item.
	I. It shall identify the method that shall be adopted for the secure return, destruction or disposal of the shared data and the timeline therefor.	The MOA/MOU should have provision/s on this item.
	J. It shall specify any other terms or conditions that the parties may agree on.	The MOA/MOU should have provision/s on this item.
Online Access	Where a government agency grants online access to personal data under its control or custody, such access must be done via a secure encrypted link. The government agency concerned must deploy middleware that shall have full control over such online access.	The AMLC is required to implement this requirement.

	Requirement	Remarks
Transfer of Personal Data	Where a data sharing agreement involves the actual transfer of personal data or a copy thereof from one party to another, such transfer shall comply with the security requirements imposed by the Act, its IRR, and all applicable issuances of the Commission.	The AMLC is required to implement this requirement.
Responsibility of the Parties	All parties to a data sharing agreement shall comply with the Act, its IRR, and all applicable issuances of the Commission, including putting in place adequate safeguards for data privacy and security. The designated data protection officer shall be accountable for ensuring such compliance. In the case of a government agency, the head of agency shall be responsible for complying with the security requirements provided in the Act, its IRR and all applicable issuances of the Commission	The AMLC is required to implement this requirement.
Accountability for Cross-border Transfer of Personal Data	Each party to a data sharing agreement shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation	The AMLC is required to implement this requirement.
Security of Personal Data	Data sharing shall only be allowed where there are adequate safeguards for data privacy and security. The parties to a data sharing agreement shall use contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred.	The AMLC is required to implement this requirement.
Review by the Commission	A data sharing agreement shall be subject to a review by the Commission, on its own initiative or upon a complaint by a data subject.	The subject MOAs/MOUs may be subjected to review by the Commission.
Mandatory Periodic Review	The terms and conditions of a data sharing agreement shall be subject to a mandatory review by the parties thereto upon the expiration of its term, and any subsequent extensions thereof. The parties shall document and include in its records:	The AMLC is required to implement this requirement.

	Requirement	Remarks
	A. reason for terminating the agreement or, in the alternative, for renewing its term; and B. in case of renewal, any changes made to the terms and conditions of the agreement.	
Termination	A data sharing agreement may be terminated: A. upon the expiration of its term, or any valid extension thereof; B. upon the agreement by all parties; C. upon a breach of its provisions by any of the parties; or D. where there is disagreement, upon a finding by the Commission that its continued operation is no longer necessary, or is contrary to public interest or public policy. Nothing in this Section shall prevent the Commission from ordering *motu proprio* the termination of any data sharing agreement when a party is determined to have breached any of its provisions, or when the agreement is in violation of the Act, its IRR, or any applicable issuance by the Commission.	This provision may be applicable to the MOAs/MOUs, which in addition to the current instances where the AMLC terminates such agreements.
Return, Destruction, or Disposal of Transferred Personal Data	Unless otherwise provided by the data sharing agreement, all personal data transferred to other parties by virtue of such agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement.	This provision may be applicable, taking into consideration current AMLC policies and issuances on the matter.
Penalties	Violations of these Rules shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines in accordance with the schedule to be published by the Commission. Failure to comply with the provisions of this Circular may be a ground for administrative and disciplinary sanctions against any erring public officer or employee in accordance with existing laws or regulations.	This is applicable to the AMLC.

	Requirement	Remarks
	The commencement of any action under this Circular is independent and without prejudice to the filing of any action with the regular courts or other quasi-judicial bodies.	
Transitory Period	Upon the effectivity of this Circular, all existing data sharing arrangements shall be reviewed by the concerned parties to determine compliance with its provisions. Where an existing data sharing arrangement is not covered by any written contract, joint issuance, or any similar document, the parties thereto shall execute or enter into the appropriate agreement pursuant to the provisions of this Circular. Where an existing data sharing agreement is evidenced by a contract, joint issuance, or any similar document, but fails to comply with the provisions of this Circular, the parties thereto shall make the necessary revisions or amendments. An existing data sharing agreement found to be compliant with this Circular, except for the requirements set out in Section 4 (Consent) hereof, shall be allowed to continue until the expiration of such agreement or within two (2) years from the effectivity of this Circular, whichever is earlier, subject to the immediately succeeding paragraph: *Provided*, that any renewal or extension of such agreement shall comply with all the provisions of this Circular. In all cases, the personal information controller that collected the personal data directly from the data subjects shall, at the soonest practicable time, notify and provide the data subjects whose personal data were shared or transferred without their consent with all the information set out in Section 4 (Consent) of this Circular: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification: *Provided, further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the data sharing agreement.	The AMLA is required to duly review all existing MOAs and MOUs.

	Requirement	Remarks
	If an existing data sharing arrangement is not for the purpose of performing a public function or providing a public service, the parties thereto shall immediately terminate the sharing or transfer of personal data. Any or all related contracts predicated on the existence of such arrangement shall likewise be terminated for being contrary to law.	

As to data sharing arrangements pursuant to requests for assistance from a foreign state, the United Nations and other international organizations, we understand that there are pro-forma forms or agreements which may no longer be amended. We defer to the wisdom of the AMLC in how to best harmonize the requirements of the DPA vis-à-vis these arrangements, always taking into consideration the principles of mutuality, reciprocity and international comity.

For your reference.

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman