Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2020-032[1]

10 August 2020

[redacted]

RE: THE USE OF BLOCKCHAIN TECHNOLOGY FOR THE PHILIPPINE PERSONAL PROPERTY SECURITY REGISTRY

Dear [redacted]

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought guidance on the use of blockchain technology to store personal information obtained from clients by the Land Registration Authority (LRA) in the creation of the Philippine Personal Property Security Agency (Registry), and if such practice is in conformity with the provisions of the Data Privacy Act of 2012[2] (DPA) and its Implementing Rules and Regulations (IRR).

We understand that the LRA is mandated under Republic Act (RA) No. 11057, also known as the Personal Property Security Act (PPSA) to establish a centralized, online notice-based registry where notices relating to transactions on personal property may be registered.

You further disclosed that the LRA has taken into consideration the provisions of the PPSA and its IRR, the different functional requirements of the members of the PPSA Technical Working Group and international best practices set by the United Nations Commission on International Trade Law (UNCITRAL) in designing the Registry, which shall be using blockchain technology to store information obtained from the data subjects.

Processing of personal information; functions of public authority; statutory mandate

[1] Tags: Personal Property Security Act; public authority; special cases; general data privacy principles; blockchain technology; immutability; personal information controller; data subject rights.
[2] An Act Protecting the 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).

The DPA and its IRR provide for a list of specific information or special cases wherein the law and the rules are not applicable. In particular, Section 5(d) and the last paragraph of the said section in the IRR provides:

> "Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law…
>
> xxx xxx 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.[3]

For the said exception to apply, the following must be established:

1. Information is necessary in order to carry out the law enforcement or regulatory function of a public authority;
2. Processing is for the fulfillment of a constitutional or statutory mandate;
3. Applies only to the minimum extent of collection, access, use, disclosure or other processing necessary for the purpose; and
4. Strict adherence to all substantive and procedural processes.[4]

RA No. 11057 and its IRR provide that an electronic registry shall be established and administered by the LRA. The Registry shall provide the public an electronic means for registration and searching of registered notices relating to transactions on personal property.[5] Registered notices, which shall be part of the Registry and considered as public records, shall contain personal information such as the names of grantors, borrowers and creditors for identification purposes.[6]

The respective contact information of the grantors, borrowers and creditors such as addresses, email addresses and mobile and phone numbers shall also be collected during the online registration process for notification purposes, but shall not be disclosed to the public.[7]

Taking these into consideration, the collection and subsequent disclosure of personal information through the Registry is necessary in the exercise of the LRA's regulatory mandate. The information necessary for the said mandate falls outside the scope of the DPA, but only to the minimum extent necessary to achieve LRA's purpose which is the implementation and administration of the Registry.

---

[3] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) and last ¶ (2016).
[4] See generally: National Privacy Commission, NPC Advisory Opinion No. 2018-079 (Oct. 23, 2018).
[5] An Act Strengthening the Secured Transactions Legal Framework in the Philippines, Which Shall Provide for the Creation, Perfection, Determination of Priority, Establishment of a Centralized Notice Registry, and Enforcement of Security Interests in Personal Property, and For Other Purposes [Personal Property Security Act], Republic Act No. 11057, § 26 (b) (2018).
[6] Rules and Regulations Implementing the Personal Property Security Act, § 5.05 (a) (2018).
[7] As disclosed by the LRA in the attachment to its letter request: *Annex B-PPSA_Discussion Sheet_ Data Inventory and Data Privacy_01 (2020.05.07)*.

Adherence to the general data protection principles; security measures

We note that, although there is legal basis for the LRA to process personal information pursuant RA No. 11057, the LRA must still adhere to the other requirements of the DPA with regard to the protection of personal information and the rights of data subjects.

As a personal information controller, the LRA must adhere to the general data privacy principles of transparency, proportionality and legitimate purpose.

To uphold transparency, it is recommended that there be a privacy notice to the data subjects. i.e. prior to the filling out of information, such notice may be provided wherein details, such as but not limited to, the legal basis for the processing, the manner in which the data will be used and stored, which information are mandated to be available for public access and information which will be stored, although not disclosed to the public. This way, the data subjects will be aware of how their information will be used and the consequences involved therein.

During the online registration process, LRA must collect only such personal information that are necessary and not excessive to achieve its mandate. Further, organizational, technical, and physical security measures in the management of the personal information collected for the Registry should be implemented. Should a third-party service provider be engaged, the arrangement must be covered by an appropriate agreement which shall clearly define the rights, obligations, and liabilities of the parties.

Blockchain technology; personal information controller; data subject rights

A blockchain is "a shared and synchronised digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database). Blockchains are designed to achieve resilience through replication, meaning that there are often many parties involved in the maintenance of these databases."[8]

As you already mentioned in your letter, an inherent feature of blockchain technology is the immutability of the data stored. Immutability, or irreversibility, is a fundamental blockchain property that stems from the fact that transactions cannot be edited or deleted once they are successfully verified and recorded into the blockchain.[9]

Due to the above inherent characteristics of blockchain technology, there may be certain concerns as to the interplay of this technology with the provisions of the DPA, specifically on the concept of personal information controller (PIC) as well as the exercise of data subject rights.

Under the DPA, a PIC is a natural or juridical person who controls the collection, holding, processing or use of personal information. Such PIC is primarily responsible for personal

[8] Finck, Michèle, European Parliamentary Research Service, Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?, *available at* https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU%282019%29634445_EN.pdf, p. I (last accessed Aug. 10, 2020).
[9] Politou, Eugenia & Casino, Fran & Alepis, Efthymios & Patsakis, Constantinos, Blockchain Mutability: Challenges and Proposed Solutions (2019), *available at* https://arxiv.org/pdf/1907.07099.pdf, p. 5 (last accessed Aug. 12, 2020).

information under its control and accountable for complying with the requirements under the law.[10]

With blockchain technology, it seems that there may be ambiguity on who are the actual PICs – it may be possible that in this scenario, the PIC is not just LRA depending on the relevant technical and governance designs of the technology to be used,[11] and/or agreements to be executed.

Further, there are various specific rights of data subjects under the DPA. Among these rights are the right to correct any erroneous or inaccurate data, and the right to erasure of any data whenever the requirements set by the DPA have been met.[12] We note also that RA No. 11057 itself also allows for the correction of administrative errors or omissions made by the Registry.[13] But with the immutability of the data, requesting for correction or erasure can be challenging, if not impossible.

In a study for the European Parliamentary Research Service[14] on blockchain and compliance with the EU General Data Protection Regulation[15] (GDPR), these two issues were discussed in this wise:

> "First, the GDPR is based on the underlying assumption that in relation to each personal data point there is at least one natural or legal person – the data controller – that data subjects can address to enforce their rights under EU data protection law. Blockchains, however, often seek to achieve decentralisation in replacing a unitary actor with many different players. This makes the allocation of responsibility and accountability burdensome, particularly in light of the uncertain contours of the notion of (joint)-controllership under the Regulation. … Second, the GDPR is based on the assumption that data can be modified or erased where necessary to comply with legal requirements such as Articles 16 and 17 GDPR. Blockchains, however, render such modifications of data purposefully onerous in order to ensure data integrity and increase trust in the network ..."

The above concerns are likewise pertinent to our own law. The DPA imposes various obligations to PICs and provides for the rights of data subjects as discussed above.

The NPC recognizes the role of technological advancements given that it is a state policy that the fundamental human right to privacy is protected while ensuring the free flow of information to promote innovation and growth.[16]

As a regulator, however, we are technology-neutral and do not prescribe nor recommend a specific type of technology to be used by PICs who have the expertise and knowledge to select the most appropriate tools for their respective objectives and needs that are still in conformity with the mandates of the DPA. We reiterate that although technology-neutral, the NPC still

[10] Data Privacy Act of 2012, § 21.
[11] See: Finck, Panel for the Future of Science and Technology, European Parliamentary Research Service, *supra* note 8, p. 43.
[12] Data Privacy Act of 2012, § 16 (d) and (e).
[13] Rules and Regulations Implementing the Personal Property Security Act, § 5.19.
[14] See: Finck, Panel for the Future of Science and Technology, European Parliamentary Research Service, *supra* note 8, p. 101.
[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Art. 12 (5) (2016).
[16] Data Privacy Act of 2012, § 2.

requires that the implementation of such technological solutions remain complaint with the provisions of the DPA.

With this, we acknowledge that the LRA has already studied the nature of blockchain technology vis-à-vis the requirements of the PPSA and the Registry, and has taken into consideration that the use thereof has its advantages such as the security of transactions and the ease of collecting and storing data.

But in order to ensure accountability of the pertinent PIC and to uphold the rights of the data subjects, it is essential to first determine the actual PIC under this type of arrangement. As previously stated, the use of blockchain technology causes an issue on identifying the real PIC since there are several players involved i.e. the LRA, service provider of the blockchain technology and such other entities involved in the execution of the blockchain.

To resolve this issue, LRA, along with the other participants of the proposed blockchain technology to be used for the Registry, may designate in writing on who the PIC will be or the entity responsible in upholding the rights of the data subjects. Factors which may be considered in determining the PIC are the type of involvement in the blockchain process, purpose of such participant in the processing and the type of data that will be processed by such participant, among others. In the absence of such written agreement, all participants may be considered as the PIC and their liability may be joint with respect to the blockchain process.

Another option, if technologically feasible, would be to design the blockchain technology in such a way that the number of participants in the entire process is limited. This way, it will be easier to determine the actual PICs and the respective responsibilities of each participant.

LRA may take into further consideration the conduct of a privacy impact assessment (PIA) which shall, among others, assist the LRA in the identification, assessment, evaluation and management of the risks involved in the processing of personal data using blockchain technology.[17] For a more comprehensive discussion on the conduct of a PIA, kindly refer to NPC Advisory No. 2017-03 available at https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo.2017-03.pdf.

Further, it is recommended that the blockchain technology be purposefully designed from a data privacy perspective to enable data subjects to have more control over personal data that relates to them,[18] given that privacy was never one of blockchain's original problems to be addressed as the same provides solutions on authenticity only.[19] There may be available technological approaches and solutions to address the matter of immutability vis-à-vis exercise of data subject rights, i.e. technical methods (pruning, off-chain storage, encrypted in blockchain), as well as cryptographic and other advanced methods aiming at conditionally removing the immutability of the blockchain.[20]

We note that it is important to fully document all processes and design of the software, including changes thereto, to make it easier to identify the possible technological issues which may be encountered and the options available in resolving them.

[17] National Privacy Commission, Guidelines on Privacy Impact Assessments, NPC Advisory No. 2017-03 (July 31, 2017).
[18] See: Finck, Panel for the Future of Science and Technology, European Parliamentary Research Service, *supra* note 8, p. 101.
[19] See: Politou, et. al., *supra* note 9, p. 4, citing V. Buterin, Privacy on the blockchain, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ (2016).
[20] *Id.* p. 6-7, 10.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner