



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-005**

05 February 2018



**Re: DATA SHARING AGREEMENT/ DATA PROTECTION
OFFICER**

Dear ,

This refers to your query received by the National Privacy Commission (NPC) via email. You stated that your company, Doxcheck, is involved in the online verification of documents through your website and mobile app.

We understand that the “Doxcheck Document Security System provides a secure and verifiable technology in the protection of documents. The system boasts multi-tier safeguards and a robust uptime of at least 99.9%. The secure, and flexible system is hosted on a distributed cloud architecture. This enables institutions to immediately and reliably protect and verify high-value documents 24/7.”¹

Specifically, your questions pertain to the following:

- a. Is Doxcheck required to submit its data sharing agreements to the NPC for approval?
and
- b. Is the Data Protection Officer (DPO) position a different job title/position in the company or can one person have two positions/titles in the company?

Data Sharing Agreement vis-à-vis Outsourcing Agreement

The Implementing Rules and Regulations (IRR) of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA), lays down the principles for data sharing² and outsourcing.³

To clarify, *data sharing* is the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or personal information processor (PIP). In the case of the latter, such disclosure or transfer must have been upon the instructions of the

¹ FAQs, <https://www.doxcheck.com/faqs/> (last accessed 30 January 2018).

² IRR of RA No. 10173, §20.

³ Id., §43-44.

PIC concerned. The term excludes *outsourcing*, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.⁴

Our understanding of the processing activities of Doxcheck is that it provides “a unique DOXCHECK Global Code is assigned to every document using a 2048-bit data security encryption.”⁵

The protected document itself is issued by “any institution/organization that issues high value documents such as: IDs, Birth Certificates, Training Certificates, Diploma, Transcript of Records, Membership Certificates, Membership Cards, Certificate of Employment, Medical Certificates, Authorization Letter, Good Moral, Any High Value Documents.”⁶

Hence, Doxcheck is a PIP to whom PICs outsourced the processing, i.e. security and protection, of the documents which may contain personal data.⁷

Section 44 of the IRR provides that processing by a PIP shall be governed by a contract or other legal act that binds the PIP to the PIC. This agreement for outsourcing is not required to be submitted to the NPC for its approval prior to its execution. Note however that said document may be required for submission by the NPC in case of a compliance check or an investigation.

In the same manner, the IRR does not require the submission of data sharing agreements to the NPC for its approval. Bear in mind, however, the IRR requires, among others, that such data sharing agreements shall be subject to the review by the NPC, on its own initiative or upon complaint of the data subject concerned.⁸ Hence, the NPC has the right to require the submission of such data sharing agreements should it deem necessary.

Data Protection Officer

As regards your query on the DPO, the NPC issued *NPC Advisory No. 2017-01 – Designation of Data Protection Officers* which sets out the guidelines on the designation of a DPO applicable to all who are engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR and the issuances of the NPC.

Pursuant to said Advisory, a DPO should be a full-time or organic employee of the PIC or PIP, occupying a regular or permanent position. To fully carry out the spirit and purpose of the law, the DPO shall act independently in the performance of his or her functions and shall enjoy sufficient degree of autonomy.

In his or her capacity as DPO, he or she may perform (or be assigned to perform) other tasks or assume other functions, however, such tasks and functions should not give rise to any conflict of interest.⁹

⁴ IRR of RA No. 20173, §3(f).

⁵ FAQs, <https://www.doxcheck.com/faqs/> (last accessed 30 January 2018).

⁶ Id.

⁷ RA No. 10173, §3(i).

⁸ IRR of RA NO. 10173, 20(b)(2)(b).

⁹ NPC Circular No. 2017-01, “Conflict of Interest” refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO. This includes, inter alia, holding a position within the PIC or PIP that leads him to determine the purposes and the means of the processing of personal data. The term shall be liberally construed relative to the provisions of this Advisory.

Given the foregoing, an individual currently holding a position within the company may be designated as the DPO. However, it is paramount that his or her tasks or functions do not give rise to any conflict of interest against the responsibilities of a DPO.

Note that the company is not precluded from creating a separate position for the DPO, or even a distinct Data Protection Office, should it determine that the same is reasonable and appropriate vis-à-vis the risk of its processing operations.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman