PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2024-014[1]

25 November 2024

[redacted]

Re: DISCLOSURE OF INDIVIDUALS' NAMES IN RELATION TO THE REGISTRATION AND USE OF FAKE NATIONAL IDENTIFICATION CARDS

Dear [redacted]

We respond to your request for an Advisory Opinion on the propriety of disclosing the names of individuals in connection with their registration with the Philippine Statistics Authority (PSA) for the issuance of national identification cards (national IDs), including the reported use of fake national IDs.

We understand that the PSA intends to publicly post the names of hundreds of thousands of applicants and/or registered persons whose national IDs were undelivered due to change of address, including those with errors in the capture of their biometric information during registration. The PSA, pursuant to its mandate to deliver the national IDs, communicated with the applicants/registered persons through their registered mobile numbers, conducted house-to-house visits, and even sought assistance from the respective barangay officials. However, considering that the mobile number is merely optional in the application form, most of the concerned applicants/registered persons did not list down one in their forms. Thus, the PSA is proposing to post the names of these applicants/registered persons on its website and registration centers to complete their registration for the issuance of their national IDs and for the undelivered national IDs to be claimed.

Furthermore, the PSA also inquired as to whether providing the relying parties with a list of individuals who were reported to have presented fake national IDs during transactions with various government agencies and/or financial institutions is in accordance with the provisions of Republic Act No. 10173, also known as the Data Privacy Act of 2012[2] (DPA).

[1]Tags: mandate; processing of personal information; general data privacy principles; personal data protection.
[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.

We note that a relying party[3] refers to a service provider who relies on any PhilSys-enabled service, such as authentication or any other process that identifies and verifies the identity of their customers. Thereafter, a registered relying party submits to the PSA the PhilSys Number (PSN)[4] of an individual for authentication. In addition, the relying party is obliged to conform with the standards and guidelines set by the PSA, in consultation with DICT to ensure the security, efficiency, and integrity of the authentication process.[5]

Under the IRR of the Republic Act No. 11055,[6] also known as the Philippine Identification System Act (PhilSys Act), the presentation of the national ID shall constitute as sufficient proof thereof, subject to proper authentication.[7] Aside from the PSA, the general public and all relying parties may check and verify the authenticity of a national ID through the PhilSys Check, an offline identity authentication tool in the form of a website. However, any entity requesting authentication via PhilSys Check must obtain the cardholder's consent.[8]

Processing of personal information; publication of names of individuals

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.[9]

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.[10] Under the DPA, names that directly identify an individual are considered as personal information.

Accordingly, the intended posting and/or disclosure of names constitutes processing,[11] which should comply with the provisions of the DPA, particularly on the general data privacy principles. Further, the processing of such information shall be done within the limits of the PSA's mandate.

As stated in your letter-request, the PSA intends to publicly-post the names of approximately 197,470 applicants who were reported to have errors in their captured biometric information, particularly iris scan and fingerprints. The purpose of which is to recapture their biometric information. Otherwise, the PSA cannot generate a PSN for the said individuals with issues in their captured biometric information.

Section 8(D) of the Implementing Rules and Regulations (IRR) of the PhilSys Act provides:

> "*xxx*
> D. Registration Process

[3] §4(q), IRR of R.A. No. 11055.
[4] Section 7(a), Republic Act No. 11055 – *Philippine Identification System Components* – The PhilSys shall have the following key components: (a) *PhilSys Number (PSN).* - The PSN is a randomly generated, unique, and permanent identification number that will be assigned to every citizen or resident alien upon birth or registration by the PSA *xxx.*
[5] §12, 2nd par., IRR of R.A. 11055.
[6] An Act Establishing the Philippine Identification System.
[7] §12, IRR of R.A. 11055.
[8] Philippine Statistics Authority, PhilSys Check, available at https://philsys.gov.ph/philsys-check/ (last accessed 2 October 2024).
[9] §4, Republic Act No. 10173.
[10] §3(g), Republic Act No. 10173.
[11] §3(j), Republic Act No. 10173.

xxx
If the biometric and demographic information of the applicant are found to be unique, a PSN will be generated for the applicant. Otherwise, further verification shall be conducted by the PSA. **In the event that the applicant cannot be issued a PSN, he or she will be notified accordingly**.

Registration in the PhilSys is deemed successful and complete upon confirmation of registration by the PSA and the issuance of the PSN. *xxx*" *(Emphasis supplied)*

Considering the above provision and on account of the PSA's extensive efforts to contact the applicants through various means, the intended disclosure is allowed for the PSA to effectively carry out its mandate.

Secondly, the PSA has already logged 328,739 cases of undelivered national IDs tagged as return-to-sender due to change of address by the intended recipients. Thus, the PSA is contemplating to post the names of the said registered persons on its website and at the respective registration centers.

We emphasize that the PhilSys Act provides stringent safeguards for adequate protection of registered individuals' personal data, specifically under Section 17 of the Act.[12] The said provision establishes a general rule that no person may disclose, collect, record, convey, disseminate, publish, or use any information of registered persons with the PhilSys. This includes restrictions on giving access to or copies of such information to third parties or entities, including law enforcement agencies, national security agencies, or units of the AFP.

By way of exception, the personal data of persons registered with the PhilSys can be disclosed if the latter has given prior consent thereto. The consent, however, must be specific to the particular purpose for which the information is being collected for processing. Another exception is the existence of compelling interest of public health or safety. This exception, however, requires an order from a competent court, establishment of significant harm to the public, and notification to the affected parties.

Section 17 of the PhilSys Act explicitly prohibits the disclosure of personal data of individuals registered with the PhilSys, allowing exceptions only under specific circumstances to prevent unauthorized access and/or disclosure of personal data. Given these constraints, the PSA may instead consider publishing general notices or advisories about the undelivered/unclaimed national IDs with corresponding instructions on how to claim the same and/or the need to update their information with the PSA. The PSA may also consider using a secure online portal where applicants/registered persons may check the status of their national IDs.

[12] "*Section 17. Protection Against Unlawful Disclosure of Information/Records*. - No person may disclose, collect, record, convey, disseminate, publish, or use any information of registered persons with the PhilSys, give access thereto or give copies thereof to third parties or entities, including law enforcement agencies, national security agencies, or units of the Armed Forces of the Philippines (AFP), except in either of the following circumstances:
(a) When the registered person has given his or her consent, specific to the purpose prior to the processing; and
(b) When the compelling interest of public health or safety so requires, relevant information may be disclosed upon order of a competent court, provided that the risk of significant harm to the public is established and that the owner of the information is notified within seventy-two (72) hours of the fact of such disclosure. *xxx*."

Adherence to general data privacy principles; reasonable and appropriate security measures

Lastly, the PSA intends to disclose to relying parties a list of persons reported to have presented fake national IDs in transactions with various government agencies and/or financial institutions.

It is worth noting that under the PhilSys Act, it is the policy of the State to establish a single national identification system to promote seamless delivery of service, reduce corruption and curtail bureaucratic red tape, avert fraudulent transactions and misrepresentations, strengthen financial inclusion, and to promote ease of doing business.[13] Notably, the PSA is mandated to act on matters affecting the integrity and security of the PhilSys, which includes taking proactive measures against the use of fake, falsified, or altered national IDs.

As such, the disclosure of personal information to registered relying parties is allowed to avert fraudulent transactions and misrepresentations or for customer due diligence purposes, among others. However, the PSA must ensure that any disclosure of personal data aligns with the provisions of the DPA, particularly adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality, including the implementation of appropriate and reasonable security measures. Thus, the disclosure to relying parties should be limited only to the name of the individual/s appearing on the face of the national ID that is determined to be fake or counterfeit. This guarantees that the disclosure does not go beyond what is necessary to achieve the legitimate purpose of preventing fraud and ensuring the integrity of the PhilSys.

The PSA may also consider enhancing the implementation of appropriate security measures to easily detect the presence of counterfeit national IDs, thereby upholding the integrity of the national ID system.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
VIDA ZORA G. BOCAR
OIC-Director IV, Privacy Policy Office[14]

[13] §2, R.A. No. 11055.
[14] Per PCSO No. 100, s. 2024