Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2022-026[1]

23 November 2022

[redacted]

Re: DISCLOSURE OF PERSONAL DATA THROUGH THE DATABASE OF INDIVIDUALS BARRED FROM TAKING CIVIL SERVICE EXAMINATIONS AND FROM ENTERING GOVERNMENT SERVICE (DIBAR)

Dear [redacted]

We respond to your request for clarification on whether the online disclosure of personal data of dismissed officials/employees through the Database of Individuals Barred from Taking Civil Service Examinations and from Entering Government Service (DIBAR), would violate the Data Privacy Act of 2012 (DPA),[2] considering that the posting of such personal data is part of the constitutional mandate of the Civil Service Commission (CSC).

We understand that the CSC, through the Integrated Records Management Office, developed the DIBAR which is an electronic database of government officials and employees who have been dismissed and precluded from being re-hired in the government service. The DIBAR contains information on the administrative decision against the concerned officials/employees, which includes the offense committed and penalty imposed. It also contains the following: name, agency, civil service eligibility, date and place of exam, exam rating, gender, date and place of birth, occupation category, and position of the employee. This information is necessary for identity verification of a dismissed official/employee to ensure that he/she will neither be re-hired in the government service nor be able to retake any civil service examination.

[1] Tags: Civil Service Commission, constitutional mandate, exemption, disclosure, database, security measures, privacy impact assessment, proportionality, rights of data subjects, right to rectification.

[2] Republic Act (R.A.) No. 10173.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL https //www privacy gov ph Email Add info@privacy gov ph * Tel No 8234-2228

You further mentioned that the DIBAR was previously posted in the CSC Website accessible to all government agencies but was subsequently removed in 2018 as a form of self-regulation by the CSC in observance of the DPA.

Processing of personal data pursuant to a constitutional or statutory mandate; extent of exemption from the DPA

Section 4 of the DPA states that the law applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Likewise, it provides for certain exemptions, including those personal data 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.[3]

Such exemption, however, is only to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.[4] The non-applicability of the DPA or its Implementing Rules and Regulations (IRR) do not extend to personal information controllers (PICs) or personal information processors (PIPs), who remain subject to the requirements of implementing security measures for personal data protection.[5] Thus, for the exemption to apply, the personal data processed by public authorities must be necessary to carry out their function as a law enforcement agency or regulatory body, and that such processing is in accordance with their constitutional or statutory mandate.

The CSC, as the central personnel agency of the government, is constitutionally mandated to establish a career service and adopt measures to promote morale, efficiency, integrity, responsiveness, progressiveness, and courtesy in the civil service. It shall strengthen the merit and rewards system, integrate all human resources development programs for all levels and ranks, and institutionalize a management climate conducive to public accountability.[6]

We recognize that in order to uphold the principle of merit and fitness in the government service, the CSC has to establish a system for the selection and retention of those who are found to be qualified and the exclusion of those who have been adjudged unfit to hold government office due to having been dismissed for cause from the government service. Hence, it is within the CSC's mandate to develop and utilize the DIBAR for the purpose of identity verification of dismissed officials/employees for the use of all government agencies, and the same is treated as a special case under Section 5 (d) of the IRR of the DPA.

Implementation of security measures

We nonetheless underscore that as a PIC, the CSC is still required under the DPA to implement reasonable and appropriate organizational, physical, and technical security

[3] Data Privacy Act of 2012, § 4 (e); Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016), § 5 (d).
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, § 5.
[5] Ibid.
[6] PHIL. CONST. art. 9 (B) § 3; See also Executive Order No. 292, Book V, Title I, Subtitle A, Chapter 1, § 1.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL https //www privacy gov ph Email Add info@privacy gov ph * Tel No 8234-2228

measures for the protection of personal data within its custody.[7] The security measures shall maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any unlawful processing.[8]

This obligates the CSC to ensure that any natural person acting under their authority and who has access to personal data in the DIBAR, processes the data contained therein only upon proper instruction or as required by law.[9] The CSC should limit the access to DIBAR only to specific authorized users whose functions necessitate such access, such as the designated personnel from the Human Resource (HR) department/division of government agencies.

It is also incumbent upon the CSC to establish and implement data protection policies specific for the DIBAR, taking into account the nature, scope, context, and purposes of the processing, as well as the risks posed to the rights and freedoms of the dismissed officials/employees who are the data subjects.[10] For further information on security measures for the protection of personal data, please refer to Sections 25-29 and 30-33 of the IRR of R.A. No. 10173.

Privacy impact assessment

We also highlight that all sensitive personal information in the DIBAR should be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to the IRR and other issuances of the National Privacy Commission (NPC).[11] CSC should conduct a Privacy Impact Assessment (PIA) prior to the adoption of the DIBAR. In CID Case No. 17-K-003, we discussed the following:

> "A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.
>
> To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization's Privacy Management Program (PMP)."

For further guidelines, please refer to NPC Circular No. 2016-01 - Security of Personal Data in Government Agencies and NPC Advisory No. 2017-03 - Guidelines on Privacy Impact Assessments.

Adherence to general data privacy principles; proportionality

[7] Rules and Regulations Implementing the Data Privacy Act of 2012, § 25.
[8] Ibid.
[9] Ibid.
[10] Rules and Regulations Implementing the Data Privacy Act of 2012, § 26 (b).
[11] *Id.* § 30-33.

In the implementation of the DIBAR, the CSC should also adhere to the general data privacy principles provided under the DPA and its IRR, particularly the principle of proportionality.

The CSC must ensure that the disclosure of personal data to the government agencies, through the DIBAR, is limited to the declared and specified purpose. Similarly, only those personal data that are adequate, relevant, suitable, necessary, and not excessive in relation to the purpose should be disclosed.

As such, personal data disclosed to the authorized users should be limited to information necessary to verify the identity of the dismissed officials/employees. The CSC should determine and evaluate whether all the personal data indicated are indispensable for the purpose of ascertaining the identity of those included in the DIBAR. Likewise, the DIBAR should not be publicly accessible online, considering that the information stated therein may be considered sensitive personal information, particularly those involving the offense committed by the concerned officials/employees and the penalty imposed.

Fair and accurate processing; limitations on data subject rights

In addition, the CSC has the obligation to ensure that all personal data are processed fairly and lawfully, and are accurate, relevant and, kept up to date.[12] In case of inaccurate or incomplete personal data in the DIBAR, the same must be rectified, supplemented, destroyed or their further processing restricted by the CSC.[13]

The CSC should also provide means for the exercise of data subject rights. However, we emphasize that these rights are not absolute and may be duly restricted when necessary for public interest, protection of other fundamental rights, or when the processing of personal data is for investigations in relation to any criminal, administrative, or tax liabilities of a data subject, among others.

Considering the foregoing, we clarify the minimum requirements and recommend the following:

- Since the DIBAR was developed only for the use of all government agencies, CSC shall not provide access to the public, even though it is made available on its website. For this purpose, the CSC may update the DIBAR by incorporating an identity verification of the authorized users, such as requiring a username and password and other Multi-Factor Authentication (MFA) methods.
- Only authorized HR personnel from government agencies shall be given access to the DIBAR.
- There should be adequate safeguards to protect CSC's computer network against accidental, unlawful or unauthorized usage, or any interference which will affect data integrity or hinder the functioning or availability of the DIBAR.
- Prior to the adoption of the DIBAR, CSC should conduct a PIA.
- The CSC should have available mechanisms for the exercise of the rights of the data subjects where applicable, such as the right to rectification.

[12] Data Privacy Act of 2012, § 11 (b) (c).
[13] Ibid.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL https //www privacy gov ph Email Add info@privacy gov ph * Tel No 8234-2228

We trust that the CSC is aware of its obligations under the DPA, its IRR, and issuances of the NPC, such as NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies and NPC Circular No. 16-03 on Personal Data Breach Management, among others.

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.

Please be guided accordingly.

Very truly yours,

SGD.
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL https //www privacy gov ph Email Add info@privacy gov ph * Tel No 8234-2228