Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2022-01

DATE	:	**04 February 2022**
SUBJECT	:	**GUIDELINES ON REQUESTS FOR PERSONAL DATA OF PUBLIC OFFICERS**

WHEREAS, the right to privacy, which includes information privacy, is constitutionally protected and accorded recognition independent of its identification with liberty, and at the same time, Article II, Section 11 of the Constitution emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Article II, Section 28 of the Constitution provides that the State adopts and implements a policy of full public disclosure of all its transactions involving public interest subject to reasonable conditions prescribed by law;

WHEREAS, Article III, Section 7 of the Constitution recognizes the right of the people to information on matters of public concern, where access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law;

WHEREAS, Article XI, Section 1 of the Constitution provides that public office is a public trust, and that public officers and employees must, at all times, be accountable to the people, serve them with utmost responsibility, integrity, loyalty and efficiency; act with patriotism and justice, and lead modest lives;

WHEREAS, Section 2 of Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012 (DPA) provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;

WHEREAS, Section 4 of the DPA states that the law applies to the processing of all types of personal information and to any person involved in personal information processing, but provides that the Act will not apply to specified information, including those information processed for purposes of allowing public access to information that fall within matters of public concern;

WHEREAS, the inclusion of the right to information in the Constitution is a recognition of the fundamental role of free and open exchange of information in a democracy meant to enhance transparency and accountability in government;

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

WHEREAS, Section 3, Executive Order (EO) No. 2, s. 2016 provides that every Filipino shall have access to information, official records, public records and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development;

WHEREFORE, in consideration of the foregoing premises, the National Privacy Commission (NPC) hereby issues this Advisory on the Guidelines on Requests for Personal Data of Public Officers.

SECTION 1. ***Scope and Purpose***. ―This Advisory applies to all requests for personal data about public officers, including personal data about an individual who is or was performing service under contract for the government that relates to the services performed, and provides a set of guidelines on evaluating such requests: *provided*, that nothing in this Advisory shall be construed as limiting the access to, or disclosure of, any personal data that is already required by law or regulation, specifically those relating to the lawful investigation and prosecution of offenses committed by public officers.

SECTION 2. ***Definition of Terms***. ― Whenever used in this Advisory, the following terms shall have their respective meanings as hereinafter set forth:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

B. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so;

C. "Data Subject" refers to an individual whose personal, sensitive personal or privileged information is processed;

D. "EO No. 2" refers to Executive Order No. 2, s. 2016 entitled "Operationalizing in the Executive Branch the People's Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor";

E. "Government" refers to the National Government, the local government units, and all other instrumentalities, agencies or branches of the Republic of the Philippines including government-owned or controlled corporations, and their subsidiaries;

F. "Official record" refers to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty;

G. "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;

H. "Personal information controller" or "PIC" refers to a person or organization who controls the collection, holding, processing, or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer, or disclose personal information on his or her behalf. The term excludes:

   a. a person or organization who performs such functions as instructed by another person or organization; or
   b. an individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family or household affairs.

   There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

I. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

J. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

K. "Public Officer" refers to those individuals in public service, including elective and appointive officials and employees, permanent or temporary, whether in the career or non-career service, including military and police personnel, whether in the classified or unclassified or exempt service receiving compensation, even nominal from the government;

L. "Public Record" refers to information required by laws, executive orders, rules or regulations to be entered, kept, and made publicly available by a government office;

M. "Requesting Party" refers to the natural or juridical person formally requesting personal data relating to a public officer;

N. "Sensitive personal information" refers to personal information:

   1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
   2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
   3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
   4. Specifically established by an executive order or an act of Congress to be kept classified.

SECTION 3. ***General principles***. — This Advisory is governed by the following principles:

A. The right to information on matters of public concern is imperative for transparent, accountable, collaborative, and participatory governance. This right is a key factor for effective and reasonable public participation in social, political, and economic decision-making.

B. Filipino citizens have the right to information on the data relating to public officers' positions or functions in government, which includes those that involve the discharge of their official public duties and functions.

C. Public officers are data subjects within the purview of the Act, with all the concomitant rights and available redresses under the same. However, certain personal data relating to their positions and functions is subject to certain exceptions provided in the Act and disclosures required under other applicable laws.

   In these exceptional cases, these information relating to their position and official functions are not covered by the DPA.[1] However, the exemption is not absolute. The exclusion of such information from the scope of the law is interpreted as an exemption from complying with the requirements of Sections 12 or 13 on lawful criteria for processing; and the collection, access, use, disclosure, or other processing is limited to the minimum extent necessary to achieve the purpose, function, or activity concerned. Personal information controllers (PICs) undertaking the processing of such information remain to be subject to the other requirements of the DPA, including implementing security measures to protect personal data and upholding the rights of the public officers as data subjects.

SECTION 4. ***Fair and lawful disclosure***. — Government agencies shall process various documents[2] which pertain to, and contain personal data of, public officers pursuant to constitutional, statutory, or contractual requirements.

The access to, or disclosure of, these documents may be regulated, notwithstanding their nature as a public record or public document. Each government agency shall provide for certain rules or a set of criteria against which a request for such documents shall be evaluated based on the mandate or public service performed and its relevance to the requesting party.

SECTION 5. ***Obligations of government agencies as personal information controllers***. — Government agencies are considered as personal information controllers (PICs) who exercise control over the processing of personal data.

A. As PICs, they are required to comply with the provisions of the DPA, its IRR, and issuances of the National Privacy Commission (NPC), specifically adherence to the

[1] 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 [Data Privacy Act of 2012], Republic Act No. 10173, § 4 (a) (2012) and Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).

[2] National Archives of the Philippines, NAP General Circular No. 1, Rule 2 - Definitions, *Document* – refers to recorded information regardless of medium or characteristics. Frequently used interchangeably with "records" (Jan. 20, 2009).

principles of transparency, legitimate purpose, and proportionality; implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data; and uphold the rights of their employees as data subjects.

B. Every government agency is responsible for personal data under its control or custody, including personal data that have been transferred to a third party for processing.

C. All personal data maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most reasonable and appropriate standards, taking into account the provisions of NPC Circular No. 16-01 (Security of Personal Data in Government Agencies) and other applicable NPC issuances as may hereafter be issued.

SECTION 6. ***Access to information on matters of public concern***. — In line with the mandate and thrust for open government, public disclosure, and transparency of government information, personal data may be disclosed to the extent that the requested information is shown to be a matter of public concern or interest: *provided*, that the information is relevant to the subject matter of the request and disclosure is not prohibited by any law or regulation. Any disclosure of personal data shall be in accordance with the general privacy principles of transparency, legitimate purpose, and proportionality.

SECTION 7. ***Guidelines for approving requests for information***. — The government agency shall endeavor to resolve the request for information in such a way that access or disclosure shall only be to the minimum extent necessary to fulfill the declared lawful purpose of the requesting party, and shall consider the following factors:

A. *Information about public officers and individuals performing service under contract for the government may be disclosed.*

1. The fact that the individual is or was an officer or employee of, or performed service/s under contract for, a government institution;
2. The title, business address, and office telephone number of the individual;
3. The classification, salary range, and responsibilities of the position held by the individual;
4. The name of the individual on a document prepared by the individual in the course of employment or contract with the government; and
5. Other circumstances analogous to the foregoing.

B. *The purpose of the request is legitimate and not contrary to law, morals, or public policy.*

1. The purpose of the requesting party shall be evaluated. The government agency shall determine whether the information requested falls under matters of public concern and whether there is a public purpose to be served which may outweigh the protection of the rights and freedoms of the public officer as a data subject.
2. In making such determination, the following factors may be considered on whether the disclosure will include information:
   a) About an individual's personal data relating solely to the positions held, or functions in, or services performed for, the government;

b) On the proper performance of the duties and responsibilities of the individual in any specific case; or
c) Required for transparency and accountability in relation to the use of public funds.

C. *The document or information requested is not excessive in relation to the declared and specified purpose of request.*

1. The requesting party shall provide a clear and specific purpose for processing the requested document or information.
2. The document or information requested shall be disclosed only after an evaluation was made by the government agency, upon determination that the access to or disclosure of the document or information is necessary to achieve the lawful and specified purpose of the request as declared by the requesting party.

D. *The access to, and disclosure of, specific documents that contain sensitive personal information may be granted following the requirements of existing laws or regulations. If the disclosure is indispensable to the fulfillment of the declared lawful purpose of the requesting party, the same shall be subject to existing rules and regulations of the pertinent government agencies on how access may be granted.*

1. The disclosure of documents which contain sensitive personal information, not only of the concerned public officer, but also of his or her family,[3] e.g., Personal Data Sheet (PDS), Statement of Assets, Liabilities and Net Worth (SALN), 201/120 files,[4] shall only be granted if such is necessary to fulfill the declared, specified, and lawful purpose of the requesting party.
2. Upon determining that particular sensitive personal information is irrelevant or unnecessary to the fulfillment of the purpose of the requesting party, the government agency shall redact the information extraneous to the declared purpose.
   a) Redaction must be undertaken on the documents that will be released to the requesting party;
   b) Appropriate methods of redaction shall be used. Whichever method is employed, the result must ensure that the redacted information cannot be seen or deduced due to incomplete redaction;
   c) Redaction of physical copies of documents should be accomplished in such a way that redacted text cannot be made out when the document is held up to the light; and that the ends, top or bottom of the text are not visible;[5]
   d) Redaction software shall be used correctly to ensure all redactions are irreversible prior to disclosure;
   e) Black highlighting shall be used for redaction on white and pale backgrounds to make it clear to any person accessing a document that redaction has taken place; and
   f) Redactions made to documents shall be consistent and logical as to form and

[3] Refers to the parents, spouse, and children, as well as any other relative within the fourth degree of consanguinity or affinity in the government service.
[4] See: Civil Service Commission, Memorandum Circular No. 8, s. 2007 [MC No. 8, s. 2007] (May 17, 2007).
[5] See: UK National Archives, Redaction toolkit - Editing exempt information from paper and electronic documents prior to release, available at https://cdn.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf (last accessed 2 November 2021)

substance. Where personal data is redacted in one part of a document for being irrelevant, unnecessary, or extraneous to the declared purpose, such reasoning, where applicable, shall likewise apply to subsequent evaluations of what shall be redacted.

3. For SALN requests, these shall be filed with the appropriate government agency acting as the official repository of the requested SALN. The following information in the SALN form that may be irrelevant or unnecessary to the declared purpose, taking into consideration the general privacy principle of proportionality, shall be redacted:
   a) Home address of the declarant;
   b) Details of any unmarried children below eighteen (18) years of age living in declarant's household, if any, particularly their names, dates of birth, and ages;
   c) Signatures of the declarant and co-declarant; and
   d) Government-issued ID numbers of the declarant and co-declarant.

E. *The dignity, safety, and security of the public officer shall be given due consideration.* The government agency shall be circumspect in the disclosure of documents and information as these may have implications on the dignity, safety, and security of the public officer. This factor shall always be given due consideration in evaluating all requests for information.

SECTION 8. ***Grant or denial of request***. — Government agencies shall have mechanisms in place for the management of requests that may involve the agencies' designated data protection officers and FOI decision makers.

A. If the government agency decides that the disclosure is warranted, taking Section 7 of this Advisory into consideration, the document or information may be given in the most appropriate format as determined by the said agency, i.e., paper, electronic form, etc.

B. If the requested document or information is not of public concern, or the disclosure will be detrimental to the fundamental rights and freedoms of the public officer, or is contrary to law, or analogous to those previously mentioned, the request shall be denied with justification to be provided to the requesting party.

C. The requesting party shall be informed of the decision of the government agency within a reasonable time, in accordance with applicable laws and regulations.[6] The public officer subject of the request shall also be informed of the existence of such request and the action(s) taken by the concerned government agency.

SECTION 9. ***Consent of Public Officers***. — If the requested document or information specifically relates to the personal data of a public officer, but existing laws or regulations do not require disclosure, the public officer may nevertheless consent to the disclosure of his or

[6] See: An Act Promoting Ease of Doing Business and Efficient Delivery of Government Services, mending for the purpose, Republic Act No. 9485, Otherwise known as the Anti-Red Tape Act of 2007, And For Other Purposes [Ease of Doing Business and Efficient Government Service Delivery Act of 2018], Republic Act No. 11032, § 9 (b) (2018) and Office of the President, Operationalizing in the Executive Branch the Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor, Executive Order No. 2 [E.O. No. 2] § 9 (d) (July 23, 2016).

her personal data: *provided*, that consent shall be strictly construed in favor of the data subject:

A. The government agency has the responsibility to adequately demonstrate that the consent obtained was indeed freely given, informed, specific, indication of will of the public officer; and
B. The government agency shall be accountable for the consent mechanisms it has implemented. It shall keep records of consent forms or its equivalent, showing how and when consent was obtained, and the information provided to the public officer at the time the consent was obtained.[7]

Notwithstanding the foregoing, the public officer may nevertheless disclose or release his or her own personal data directly to the requesting party without any intervention from the government agency.

SECTION 10. ***Interpretation.*** — Any doubt in the interpretation of any provision of this Advisory shall be liberally interpreted in a manner mindful of the rights and interests of the data subject.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

[7] See generally: European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, § 108 (4 May 2020), available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (last accessed 11 Sept 2021).