NPC Advisory No. 2024 – 04

DATE   :   **19 December 2024**

SUBJECT   :   **GUIDELINES ON THE APPLICATION OF REPUBLIC ACT NO. 10173 OR THE DATA PRIVACY ACT OF 2012 (DPA), ITS IMPLEMENTING RULES AND REGULATIONS, AND THE ISSUANCES OF THE COMMISSION TO ARTIFICIAL INTELLIGENCE SYSTEMS PROCESSING PERSONAL DATA**

WHEREAS, Section 7 (g) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) empowers the National Privacy Commission (NPC) to publish, on a regular basis, a guide to all laws relating to data protection;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) empowers the NPC to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Artificial Intelligence (AI) systems, which are dynamic and continuously evolving, are designed to perform tasks that require human intelligence, with or without human intervention, using techniques that enable machines to learn from data, perceive environments, process and adapt to new inputs, manipulate or generate output, and make decisions or predictions based on a set of defined objectives;[1]

WHEREAS, the DPA, its IRR, and the issuances of the Commission, which are principles-based and technology-neutral, apply to all forms of processing of personal information and sensitive personal information (collectively, personal data);

WHEREAS, the DPA, its IRR, and the issuances of the Commission apply when the processing of personal data is involved in the development or deployment of AI systems, including its training and testing;

WHEREAS, it is necessary to provide additional guidance regarding the application of the general privacy principles and specific key concepts in the DPA, its IRR, and the issuances of the Commission insofar as the AI systems involve the processing of personal data;

---

[1] *See* Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, at 36, *available at* https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (2019); OECD Council, *Recommendation on Artificial Intelligence*, OECD/LEGAL/0449, *available at* https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (2024); ISO/IEC JTC 1/SC 42, *Information Technology – Artificial Intelligence – Artificial Intelligence Concepts and Terminology*, ISO/IEC 22989:2022, § 3.1.4, *available at* https://www.iso.org/standard/74296.html (2022); National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1 (2024), n. 1, *available at* https://doi.org/10.6028/NIST.AI.600-1.

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the Guidelines on the Application of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and the issuances of the Commission to Artificial Intelligence Systems Processing Personal Data.

SECTION 1. *Scope.* — This Advisory applies when the processing of personal data is involved in the development or deployment of AI systems, including its training and testing.

SECTION 2. *Application of the DPA.* — The obligations of Personal Information Controllers (PIC), and their Personal Information Processors (PIP), under the DPA, its IRR, and the issuances of the Commission, including adhering to the general privacy principles, upholding the rights of the data subjects, determining the appropriate lawful basis for processing, and implementing security measures, apply insofar as AI systems involve the processing of personal data.

    A. ***Transparency.*** PICs shall inform their data subjects of the nature, purpose, and extent of the processing of personal data when such processing is involved in the development or deployment of AI systems, including its training and testing.[2] PICs must be able to explain the purpose for such processing, the factors and inputs considered by such AI systems, the risks associated with the processing, the expected output of the AI systems, the impact of the AI systems on data subjects,[3] and any applicable dispute mechanisms available to their data subjects.[4] PICs shall ensure that any information on such processing is easy to access, concrete and definitive, understood by members of their target audience, and presented in a simple manner using clear and plain language while retaining necessary technical terms.[5]

    B. ***Accountability.***[6] PICs shall be accountable for the processing of AI systems and for the outcomes and consequences of such processing when personal data is involved. This accountability is imposed on the specific PIC undertaking the development or deployment of the AI system, including its training and testing. When such processing is subcontracted or outsourced, PICs shall remain accountable for the actions of their PIPs.[7]

        1. ***Demonstrable Measures.*** PICs and, in cases where the processing is subcontracted or outsourced, their PIPs, must be able to demonstrate that they have implemented effective policies and procedures to comply with the DPA, its IRR, and other issuances of the Commission. PICs must maintain the necessary documentation on

---

[2] *See* 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 § 11 (a) (2012).

[3] *Id.*

[4] *See Id.* § 16 (a), (b), & (d).

[5] National Privacy Commission, Guidelines on Consent, Circular No. 04, Series of 2023 [NPC Circ. No. 23-04], § 3 (D)(3) (07 November 2023).

[6] *See* Data Privacy Act of 2012, § 21.

[7] *Id.*

these policies and procedures, including those for AI systems that involve the processing of personal data.

2. *Governance Mechanisms.* [8] PICs shall institute appropriate and effective governance mechanisms to ensure the responsible and ethical processing of personal data in the development or deployment of AI systems, including its training and testing.

These include, but are not limited to, the conduct of Privacy Impact Assessments (PIA);[9] integration of privacy-by-design and privacy-by-default; implementation of common industry security standards; continuous monitoring of the AI systems' operations; creation of a dedicated AI ethics board; regular retraining and scrubbing of the AI systems; and mechanisms for humans to intervene in decision-making and review the output of AI systems.

a. AI systems can involve automated decision-making, and the effects of such automated decisions can pose a significant risk to the rights and freedoms of data subjects. In such cases, as an additional safeguard, PICs shall implement mechanisms to allow for meaningful human intervention carried out by persons with the necessary competence and authority.

PICs shall also implement mechanisms to allow their data subjects to question and contest automated decisions when the effect of such decisions poses a significant risk to the rights and freedoms of data subjects.[10]

b. PICs shall also be responsible for regularly monitoring the proper implementation and effectiveness of these governance mechanisms.

C. *Fairness.*[11] PICs shall ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to data subjects. As such, PICs shall implement mechanisms to identify and monitor biases in the AI systems and to limit such biases and their impact on the data subjects. PICs must consider systemic bias, human bias, and statistical bias when assessing or auditing their AI systems.

Consistent with the Principle of Fairness, PICs shall not utilize AI Washing, the practice where PICs overstate the involvement of AI systems to the detriment of their data subjects, and other deceptive practices.

D. *Accuracy.*[12] PICs must maintain the accuracy of personal data to ensure the fairness of the output of the AI systems. PICs shall implement appropriate measures to ensure that personal data utilized in the AI systems is correct and kept up to date.

---

[8] *See generally Id.* §§ 20 & 21.
[9] *See* National Privacy Commission, Security of Personal Data in the Government and the Private Sector, Circular No. 06, Series of 2023 [NPC Circ. No. 23-06], (01 December 2023).
[10] *See* Data Privacy Act of 2012, § 16.
[11] *See* National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule IV, § 19 (b) (2016).
[12] *See Id.* rule IV, § 19 (c).

E. ***Data Minimization.***[13] PICs shall exclude, by default, any personal data that is unlikely to improve the development or deployment of AI systems, including its training and testing.

F. ***Lawful Basis for Processing.*** PICs shall determine the most appropriate lawful basis under Sections 12 and 13 of the DPA prior to the processing of personal data in the development or deployment of AI systems, including its training and testing.[14]

Publicly available personal data do not lose the protection afforded by the DPA, its IRR, and the issuances of the Commission simply because it has been made public or is publicly accessible.[15] When PICs process personal data that is publicly available, they shall determine the most appropriate lawful basis under the DPA and ensure that the processing adheres to the general privacy principles.

SECTION 3. *Rights of the Data Subject.*[16] — AI systems involving the processing of personal data can have implications on the exercise of data subject rights.

PICs should implement mechanisms, which may include Privacy-Enhancing Technologies (PET), to ensure the proper exercise of data subject rights while allowing for the responsible and ethical processing of personal data in the development or deployment of AI systems, including its training and testing.

A. PICs shall implement effective mechanisms or alternative measures to give effect particularly to the right to object, the right to rectification, and the right to erasure or blocking. In such cases, PICs shall communicate to their data subjects the scope and consequences of the exercise of these rights following the Principle of Transparency. When the request is not feasible, PICs shall inform their data subjects of such fact and their reasons. Nevertheless, PICs shall implement effective mechanisms or alternative measures to carry out, as far as possible, the intended effect of these rights.

B. PICs shall ensure that their data subjects may exercise data subject rights before, during, and after the development or deployment of AI systems, including its training and testing.

C. The fact that personal data has been incorporated into data sets does not automatically make the exercise of data subject rights unreasonable. PICs' inaction towards providing mechanisms that allow for the meaningful exercise of data subject rights negates any claim that fulfilling such requests is unreasonable.

---

[13] *See Id.* rule IV, § 19 (b).
[14] Data Privacy Act of 2012, §§ 12 & 13.
[15] EA and TA v. EJ, EE and HC, NPC 17-018, 15 July 2019, at 7, *available at* https://privacy.gov.ph/wp-content/uploads/2022/09/NPC-17-018-EA-and-TA-v-EJ-Decision-2019.07.15-.pdf.
[16] *See* National Privacy Commission, Data Subject Rights, Advisory No. 01, Series of 2021 [NPC Advisory No. 2021-01] (29 January 2021).

SECTION 4. *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 subjects.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

<table>
<tr><td align="center">SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner</td><td align="center">SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner</td></tr>
</table>