



## **NPC Advisory No. 2024 – 03**

**DATE** : 17 December 2024

**SUBJECT** : **GUIDELINES ON CHILD-ORIENTED TRANSPARENCY**

**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**, Section 20 of the DPA provides that Personal Information Controllers (PIC) must implement reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data. In determining the appropriate level of security, PICs must consider the risks represented by the processing, among other factors;

**WHEREAS**, a ‘child’ refers to a person below eighteen (18) years of age or those eighteen (18) or over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation, or discrimination because of a physical or mental disability or condition;<sup>1</sup>

**WHEREAS**, children, as data subjects and rights holders, are entitled to meaningful access to information;<sup>2</sup>

**WHEREAS**, PICs or Personal Information Processors (PIP), when processing children’s personal data, should ensure that children receive extra protection. Such processing should be context-specific and principles-based;

**WHEREAS**, the NPC recognizes the need to provide children with opportunities to create and interact within a protective environment;

**WHEREAS**, the principles of “best interests of the child”<sup>3</sup> and “evolving capacities”<sup>4</sup> are the primary considerations in all actions involving children. Recognizing children as rights

---

<sup>1</sup> See An Act Providing For Stronger Deterrence And Special Protection Against Child Abuse, Exploitation And Discrimination, And For Other Purposes [Special Protection of Children Against Abuse, Exploitation and Discrimination Act of 1992], Republic Act No. 7610 § 3 (a) (1992).

<sup>2</sup> See UN Committee on the Rights of the Child (UNCRC), General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment, CRC/C/GC/25 (2 March 2021).

<sup>3</sup> See Convention on the Rights of the Child art. 3(1), *adopted* 20 November 1989, 1577 U.N.T.S. 3.

<sup>4</sup> See *Id.* art. 5.

holders with varying degrees of maturity gives full effect to their best interests and evolving capacities;

**WHEREAS**, Section 16 of the DPA provides for the data subjects' right to be informed of processing of their personal data;

**WHEREAS**, Section 11 of the DPA provides that processing personal data should adhere to the general privacy principles;

**WHEREAS**, the Principle of Transparency requires PICs to provide data subjects with the necessary information on the nature, purpose, and extent of processing, including the risks and safeguards involved, the identity of the PIC, as well as data subject rights and how these can be exercised;

**WHEREAS**, the Principle of Transparency requires that any information and communication relating to the processing of personal data should be easy to access, concrete and definitive, understood by a member of its target audience, and presented in a simple manner using clear and plain language while retaining necessary technical terms;

**WHEREFORE**, in consideration of these premises, the NPC hereby issues this Advisory on the Guidelines on Child-Oriented Transparency.

**SECTION 1. *Scope.*** – This Advisory applies to all PICs and PIPs engaged in the processing of children's personal data, whether in a digital or physical environment. It covers products or services specifically intended for children or likely to be accessed by children.

**SECTION 2. *Risk-Based Assessment.*** – The processing of children's personal data must adhere to the general privacy principles.<sup>5</sup> PICs shall ensure that, in accordance with the Principle of Transparency, children are aware of the nature, purpose, and extent of the processing of personal data. Consistent with the purpose of a Privacy Impact Assessment (PIA), PICs shall adopt a risk-based and child-oriented approach when informing children whose data they are processing, taking into account their age and the risks involved in the specific processing activity.

A. ***Privacy Impact Assessment (PIA).*** PICs must incorporate Child Privacy Impact Assessments (CPIA) as part of their PIAs before launching products or services intended or likely to be accessed by children and thereafter as may be necessary.<sup>6</sup> The PIA is a continuing requirement, regularly reviewed and updated to account for changes in products, services, processes, or regulations.<sup>7</sup> The factors that must be considered include, but are not limited to:

1. Purpose of processing;
2. Types of data to be processed (*e.g.*, collected, used, or disclosed);
3. Sources of data;
4. Systems to be used (*e.g.*, open or closed systems);

---

<sup>5</sup> 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 (2012).

<sup>6</sup> 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).

<sup>7</sup> See *Id.*

5. Data storage and disposal;
6. Data sharing;
7. Security measures implemented;
8. Effect or impact of the specific processing activity on children;
9. Age range of intended or likely users;
10. Process owner for the specific processing activity of the PIC or PIP;
11. Risk Identification; and
12. Involvement of Parents or Guardians

The involvement of parents or guardians may be necessary in determining whether children may participate in the specific processing activity, particularly when there are heightened risks to children. PICs must determine the appropriate methods for securing and verifying this involvement based on the level of risk to children.

- B. PICs should implement appropriate measures to address any risks identified in the PIA to ensure the protection of children's personal data taking into consideration the best interests of the child, and to promote the Principle of Transparency in processing activities.<sup>8</sup>

In this regard, PICs may employ the following measures, among others:

1. **Age Assurance Mechanisms.** PICs may implement age assurance mechanisms or solutions to determine the age range of their users as a tool to adopt age-appropriate practices when processing children's personal data. In determining the most suitable age assurance mechanism or solution for a specific processing activity, PICs should recognize that relying solely on users' self-declaration may be inadequate for high-risk processing activities.

PICs must ensure that children understand the purpose of the age assurance process. The processing of personal data for age assurance must adhere to the general privacy principles and must have a lawful basis for processing.<sup>9</sup>

2. **Privacy Controls.** PICs must adopt a risk-based approach to determine and implement appropriate and enhanced privacy controls when processing children's personal data, ensuring:
  - a. **High Privacy Settings by Default:** Children's accounts must have privacy settings set to the highest level by default. This includes disabling geolocation services, setting profiles to private, and minimizing data sharing unless necessary for the specific purpose.<sup>10</sup>
  - b. **Easy Access to Privacy Settings:** PICs must ensure that children are fully aware of the available privacy settings and how to adjust them. These settings should be clear, easy to access, and designed in a way that enables children to understand and control their privacy preferences while maintaining a minimum level of protection.

---

<sup>8</sup> Data Privacy Act of 2012, § 20 (f).

<sup>9</sup> See *Id.* §§ 11 - 13.

<sup>10</sup> *Id.* § 11.

**SECTION 3. *Privacy Notice.*** PICs shall ensure that children are aware of the nature, purpose, and extent of the processing of personal data.<sup>11</sup> PICs should consider the readability (e.g., vocabulary, tone, or style), comprehension, and granularity of Privacy Notices while taking into consideration the best interests and evolving capacities of children.

PICs shall ensure that the Privacy Notice, including any information and communication relating to the processing of personal data, is readily accessible, taking into consideration user experience and user interface. PICs must clearly inform children how to access any information or communication relating to the processing of their personal data.

PICs may utilize a variety of alternative formats, such as videos, infographics, animations, and audio recordings, to deliver privacy-related information to children. PICs should design these formats to ensure that the Privacy Notices are presented in a manner that is simple and easily understandable, taking into consideration the age range of the intended or likely users.

A. ***Content.*** PICs should inform the children of the following:

1. Specific and precise processing activities involving the personal data of the children;
2. Purpose of processing;
3. Appropriate lawful basis;
4. Potential consequences and risks associated with the processing of the personal data of the children;
5. Importance of privacy settings;
6. Rights as data subjects and the manner and method of exercising these; and
7. Revisions or updates to the Privacy Notice, if any.

B. ***Age-Appropriate Privacy Notice.*** PICs must ensure that any information or communication relating to the processing of children’s personal data should be concrete and definitive, and understood by intended or likely users whose personal data are involved in the specific processing activity.<sup>12</sup> PICs shall present the information in a simple manner using clear and plain language while retaining necessary technical terms.<sup>13</sup> This ensures that children receive relevant privacy-related information in a language that is appropriate and easily comprehensible, taking into consideration the age range of the intended or likely users.

In instances where the product, or service involves or contemplates children as data subjects, regardless of whether it is also intended for adults, PICs must provide child-friendly Privacy Notices in addition to standard versions.<sup>14</sup>

C. ***Just-in-time Privacy Notice.***<sup>15</sup> PICs shall provide information on how children’s personal data will be processed at the point in time when personal data is about to be processed. PICs shall ensure that the information presented is the minimum specific information relevant to the specific processing activity that will be undertaken;

---

<sup>11</sup> *Id.*

<sup>12</sup> See National Privacy Commission, Guidelines on Consent, Circular No. 04, Series of 2023 [NPC Circ. No. 23-04], § 3 (D)(3) (07 November 2023).

<sup>13</sup> *Id.*

<sup>14</sup> See *Id.* § 3.

<sup>15</sup> See *Id.* § 2 (E).

- D. **Layered Privacy Notice.**<sup>16</sup> PICs shall use Layered Privacy Notices that embody the minimum specific information for purposes of the Principle of Transparency. These should direct children to supplemental and detailed information relevant to the specific processing activity that will be undertaken. PICs shall ensure that the supplemental and detailed information presented to children is separate from that intended for adults and presented in a language that is appropriate and easily comprehensible for children;
- E. **Deceptive Design Patterns.**<sup>17</sup> PICs shall not use deceptive methods or any form of coercion, compulsion, threat, intimidation, or violence in the processing of the children's personal data.

PICs shall not use characters that children know and trust to influence them to provide more information than necessary for the specified and declared purpose. Further, PICs shall not use designs that nudge or steer children toward selecting options that compromise their privacy or are inconsistent with their best interests.

**SECTION 4. Data Breach Notification.** – In cases of data breaches that fall under mandatory breach notification according to issuances on data breach management, PICs shall notify the data subjects even if the data subjects are children.<sup>18</sup>

In cases where the affected data subjects are children, PICs shall notify both the children and their parents or guardians. When notifying children, PICs must use the appropriate language readily understandable to the children.<sup>19</sup>

PICs are not precluded from notifying children and their parents or guardians when the data breach does not fall under mandatory breach notification.

**SECTION 5. Accountability.** – PICs are responsible for the processing of children's personal data, including personal data that has been subcontracted or outsourced to their PIPs.<sup>20</sup> In all actions, PICs must place the best interests of the child as the primary consideration. As such, PICs must adopt a risk-based and context-specific approach when determining the most suitable age-assurance mechanism or solution, if any; when evaluating appropriate content for their data subjects and the manner of informing them of the specific processing activity; and when implementing appropriate and enhanced security measures, privacy controls, and safeguards.

**SECTION 6. 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 children, recognizing them as rights holders and giving full effect to their best interests and evolving capacities.

---

<sup>16</sup> See *Id.* § 3 (D)(3)(c).

<sup>17</sup> See *Id.* § 7; National Privacy Commission, Guidelines on Deceptive Design Patterns, Advisory No. 01, Series of 2023 [NPC Adv. No. 23-01] (07 November 2023).

<sup>18</sup> See NPC Circ. No. 23-04, § 11.

<sup>19</sup> See *Id.* § 3 (D)(3).

<sup>20</sup> Data Privacy Act of 2012, § 21.

Approved:

**SGD.**  
**JOHN HENRY D. NAGA**  
Privacy Commissioner

**SGD.**  
**LEANDRO ANGELO Y. AGUIRRE**  
Deputy Privacy Commissioner

**SGD.**  
**NERISSA N. DE JESUS**  
Deputy Privacy Commissioner