NPC Advisory No. 2026 - 01

DATE : **13 April 2026**

SUBJECT : **GUIDELINES ON DATA SCRAPING OF PUBLICLY AVAILABLE PERSONAL DATA**

WHEREAS, Republic Act No. 10173, also 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 the free flow of information to promote innovation and growth. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, Section 7 of the DPA provides that the National Privacy Commission (NPC) is charged with the administration and implementation of the DPA, which includes ensuring the compliance of Personal Information Controllers (PICs) and Personal Information Processors (PIPs), and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country in coordination with other government agencies and the private sector;

WHEREAS, under Section 9 (a) of the Implementing Rules and Regulations of the DPA (IRR), as amended, the NPC is mandated to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, the NPC is cognizant that organizations may use data scraping practices and technologies in processing publicly available personal data from any online source;

WHEREAS, the NPC likewise acknowledges that these data scraping practices and technologies raise data privacy concerns since such scraped data can be exploited and misused, potentially violating the DPA;

WHEREAS, the NPC reiterates that the protections afforded under the DPA, its IRR, as amended, and issuances of the NPC apply to the processing of publicly available personal data;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Advisory on the data scraping of publicly available personal data.

SECTION 1. ***Scope and Purpose.*** — This Advisory applies to and provides guidelines for PICs and PIPs that engage in data scraping practices and technologies, and PICs that host publicly available personal data which may be subject to data scraping.

SECTION 2. ***Definition of Terms.*** **—** The terms used in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Advisory, the following terms are defined as follows:

A. "Data Scraping" refers to the automated or manual process of extracting publicly available personal data, including text, images, audio and video recordings, and user profiles, from websites, applications, or other online sources. This includes using scraping tools or technologies to access websites through HTTP requests, parsing HTML content of webpages, identifying and extracting specific data elements, *e.g.,* text, images, structuring the data to remove irrelevant information, and storing it in a structured format (*e.g.,* databases or JSON files) for further analysis or use.

B. "Publicly available personal data" refers to personal data that are readily available and accessible to the public without restrictions or the need for authorization or authentication (*e.g.,* no log-in credentials required). This includes personal data required by laws or regulations to be made publicly available, as well as personal data intentionally made publicly available by data subjects themselves through public platforms such as but not limited to social media.

C. "Large-scale scraping" refers to the process of extracting substantial volumes of publicly available personal data at a frequency that exceeds routine or small-batch operations, characterized by sustained patterns of extensive HTTP requests across vast numbers of webpages. For purposes of determining whether scraping is considered large-scale, the following factors may be considered:

    1. The number of data subjects affected;
    2. The volume of data or the range of data items extracted;
    3. The duration or permanence of the data scraping activity; and
    4. The geographical extent of the data scraping activity.[1]

SECTION 3. ***Conduct of lawful data scraping.*** **—** Data scraping may be allowed: *provided*, that PICs engaged in data scraping, including those performed for and on its behalf by third parties, shall strictly fulfill their obligations under the DPA, such as but not limited to the following general requirements:

A. PICs shall clearly define the specific and legitimate purpose for scraping publicly available personal data. Such purpose shall not be contrary to law, morals, public order, or public policy. Processing shall be limited to such specified and declared purpose (*e.g.*, data matching, data enhancing, profiling, identity resolution) and shall not be used for purposes that are unrelated or not reasonably expected by data subjects.

B. PICs shall determine the most appropriate lawful basis for processing personal data obtained through data scraping, including any further disclosures of such data to third parties, under Section 12 or 13 of the DPA. The public availability of personal data does not constitute consent by the data subject to its processing for purposes beyond

[1] S*ee:* Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP 248 rev.01, at 10 (adopted 4 April 2017, last revised and adopted 4 October 2017).

those reasonably contemplated at the time it was provided, nor does it relieve a PIC of its obligations under the DPA.

C. PICs shall inform data subjects, through an appropriate privacy notice or consent form (where processing is consent-based), before the processing takes place, or at the next practical opportunity that their personal data are processed using data scraping practices and technologies in addition to the requirements of Section 3 of NPC Circular No. 2023-04.[2]

D. PICs shall ensure that scraped personal data are adequate, relevant, suitable, and necessary in relation to its purpose, and shall refrain from excessive or indiscriminate data scraping. PICs shall also assess whether data scraping is reasonable under the circumstances and whether its declared purpose/s could not be reasonably fulfilled by other less intrusive means.

E. In the design, development, or deployment of data scraping technologies, PICs shall take into consideration the reasonable privacy expectations of data subjects. They shall adopt appropriate technical, organizational, and physical security measures to protect data subjects and uphold data privacy rights, including, where applicable, the use of privacy-enhancing technologies.

F. PICs engaged in data scraping shall conduct a Privacy Impact Assessment (PIA) covering such activities, including those performed for and on its behalf by third parties.[3] The PIA shall be performed in accordance with NPC issuances and shall assess, at a minimum: (1) the nature, scope, and purpose of the intended data scraping; (2) the risks to the rights and freedoms of data subjects, including the risks from the aggregation of scraped data with other datasets; and (3) the measures to be adopted to address or mitigate such risks. The PIA shall be reviewed and updated periodically, or whenever there is a material change in the scope, purpose, or nature of the data scraping activity.

G. Data scraping involving sensitive personal information is prohibited, unless the PIC can demonstrate: (a) a valid lawful basis under Section 13 of the DPA; (b) that the collection is strictly necessary and proportional to a legitimate purpose; and (c) that enhanced technical, organizational, and physical security measures are in place.

H. Data scraping involving personal data of vulnerable data subjects,[4] including, but not limited to, minors, the elderly, and persons with disabilities, is subject to heightened scrutiny. In such cases, PICs must demonstrate that the processing does not exploit the capacity of data subjects.

---

[2] *See* National Privacy Commission, Guidelines on Consent, NPC Circular 2023-04 (07 November 2023).
[3] *See* National Privacy Commission, Security of Personal Data in the Government and the Private Sector, NPC Circular No. 2023-06, §5 (01 December 2023).
[4] Under the Supreme Court of the Philippines Code of Professional Responsibility and Accountability (A.M. No. 22-09-01-SC), a vulnerable person is a person who is at a higher risk of harm than others, and shall include children, the elderly, the homeless, persons with disability, persons deprived of liberty, human rights victims, victims of domestic violence, victims of armed conflict, those who are socio-economically disadvantaged, those who belong to racial or ethnic minorities, or those with debilitating physical or mental conditions.

SECTION 4. ***Unauthorized data scraping practices.*** **—** Data scraping is deemed unauthorized when it is conducted in violation of applicable laws, the DPA and its IRR, NPC Issuances, or the terms of service or terms of use of websites or applications. Unauthorized data scraping includes, but is not limited to, the circumvention or bypassing of technical measures implemented by websites or applications to prevent data scraping[5]. The use of deceptive design patterns, misrepresentation, or similar techniques to obtain personal data through data scraping is likewise deemed unauthorized. Unauthorized data scraping may give rise to criminal, civil, and administrative liability under the DPA, its IRR, as amended, and NPC issuances.

SECTION 5. ***Hosting publicly available personal data.*** **—** PICs whose websites, applications, or other online platforms host publicly available personal data shall take into consideration the following guidelines:

A. Data subjects shall be informed that their personal data are publicly available and may be subject to data scraping. PICs should provide clear and accessible information such as, but not limited, to the following:

    1. The categories of personal data that can be accessed through data scraping practices and technologies;
    2. Whether terms of service or terms of use permit third parties to scrape personal data, and where known, provide information on the identities of such third-party entities, the purposes of data scraping, and the intended use of the scraped data;
    3. Mechanisms by which data subjects may object to, disallow, or seek the termination of data scraping, in accordance with their rights under the DPA; and
    4. The security measures implemented to deter or mitigate unauthorized data scraping.

B. PICs shall implement reasonable and appropriate security measures to mitigate data privacy risks from data scraping, which may include the following:

    1. Conducting PIA to:
        a. Maintain an inventory of publicly available personal data and the basis for their public availability (*e.g.,* legal requirement or intentional disclosure by data subjects);
        b. Assess the risks to the rights and freedoms of data subjects arising from data scraping; and
        c. Identify measures to address or mitigate such risks.
    2. Implementing data breach notification procedures where unauthorized data scraping constitutes a notifiable personal data breach;
    3. Continuously monitoring risks and threats associated with data scraping, which may include:[6]

[5] These measures may include a robots.txt exclusion protocol or integration of CAPTCHAs, among others. *See* Commission Nationale de l'Informatique et des Libertés (CNIL), *The legal basis of legitimate interest: focus sheet on the measures to implement in the case of data collection by web scraping*, available at https://www.cnil.fr/en/legal-basis-legitimate-interest-focus-sheet-measures-implement-case-data-collection-web-scraping (last accessed 26 March 2026).

[6] See generally: Global Privacy Assembly (GPA) International Enforcement Cooperation Working Group, Joint statement on data scraping and the protection of privacy, available at https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf (last accessed: 8 August 2024).

a. Detecting automated or non-human "bot" activity patterns, such as sudden or abnormal increases in web traffic;
b. Imposing rate limits or access restrictions to prevent unauthorized or excessive automated collection of personal data;
c. Monitoring suspicious or abnormally high activity by user accounts; and
d. Blocking IP addresses or disabling accounts associated with malicious or unauthorized scraping activities.

SECTION 6. ***Accountability.*** **—** PICs remain accountable for ensuring that their data scraping practices, including those performed by PIPs, comply with the DPA, its IRR, and relevant NPC issuances.

A. PICs shall maintain documented policies, and practices governing their data scraping activities, including documentation of PIAs conducted in relation to such activities.

B. Where data scraping is conducted by a PIP, such activities shall be governed by appropriate agreements that specify adequate and necessary data privacy and security measures. Such agreements shall explicitly prohibit unauthorized data scraping and the circumvention of security measures.

C. The use of contractual or other arrangements shall not relieve PICs of their accountability under the DPA.

D. PICs shall establish policies and procedures for the periodic review and updating of authorized or conducted data scraping activities.

E. PICs shall adopt retention and disposal policies for scraped data. Personal data obtained through data scraping shall be retained only for as long as necessary to fulfill the declared purpose and shall be securely disposed of thereafter.

SECTION 7. ***Use of scraped personal data.*** **—** In using scraped personal data, PICs shall observe the following guidelines:

A. PICs that obtain personal data sourced from other PICs independently engaged in the conduct of data scraping activities shall establish policies and procedures, including the use of contractual or other reasonable means, for verifying and ensuring that personal data under this arrangement was obtained in compliance with the requirements of the DPA, its IRR, and the various issuances of the NPC, including this Advisory. To this effect, any further processing of personal data obtained through data scraping activities under Section 4 of this Advisory shall likewise be considered unauthorized.

B. PICs shall disclose, in their privacy notices, when personal data are obtained from publicly available sources, including the source of the data, the purpose of the collection, and the manner of processing.

C. In the use, analysis, or interpretation of scraped personal data, the PICs shall implement mechanisms to identify, monitor, and limit possible sources of bias, unfairness, or discriminatory treatment against data subjects.

D. PICs shall not use scraped personal data in a manner that would cause harm to the data subject, including, but not limited to:

1. Identity fraud or targeted cyberattacks;
2. Doxxing or the malicious public disclosure of personal data intended to harass or intimidate;
3. Unauthorized sale or disclosure of personal data for malicious purposes;
4. Unauthorized surveillance or intelligence gathering;
5. Large-scale scraping of social media sites for unauthorized profiling; and
6. The collection of login credentials or unauthorized access to users' accounts.

E. PICs shall not use scraped data for purposes beyond those originally declared unless:
1. An appropriate lawful basis under Sections 12 and 13 of the DPA exists;
2. Sufficient notice is given to affected data subjects;
3. A new PIA is conducted; and
4. Compliance with any other requirements under this Advisory.

SECTION 8. ***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.

ATTY. JOHANN CARLOS S. BARCENA, ***CESO III***
Privacy Commissioner

SGD.

ATTY. JOSE AMELITO S. BELARMINO II, ***MSc***
Deputy Privacy Commissioner

SGD.

ATTY. JUAN PAOLO F. FAJARDO
Deputy Privacy Commissioner