Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2022-024[1]

21 November 2022

[redacted]

Re: FREE FLOW OF DATA

Dear [redacted]

We respond to your inquiry regarding the concept of the free flow of data. You cited in your letter the discussions on the concept of "free flow of data" in high-level statements of the APEC,[2] and G20.[3] Likewise, in the WTO Joint Statement Initiative on e-commerce, the relevant working text refers to the "flow of information" as well as "cross-border transfer of information by electronic means" or "cross-border data flows."

You further inform that trade agreements have also evolved to meet changing digital realities, with provisions relating to enabling trusted data flows by developing mechanisms to protect personal data being transferred across borders and allow businesses to transfer information across borders regardless of where they are located.

It is in this context that the Bureau of International Trade Relations (BITR) of the Department of Trade and Industry (DTI) is inquiring whether the concept of the free flow of data falls

[1] Tags: free flow of data; data transfer; cross-border data transfer; accountability.
[2] APEC Internet and Digital Economy Roadmap: Key focus area of "Facilitating the free flow of information and data for the development of the Internet and Digital Economy, while respecting applicable domestic laws and regulations"; APEC Putrajaya Vision 2040: Innovation and Digitalization pillar, wherein members have committed to "strengthen digital infrastructure, accelerate digital transformation, narrow the digital divide, as well as cooperate on facilitating the flow of data and strengthening consumer and business trust in digital transactions; APEC Cross-Border Privacy Rules (CBPR) System and APEC Privacy Framework: Preamble states that "a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region."
[3] At the G20, Japan launched the Osaka Track based on the concept of "data free flow with trust" (DFFT) as an organizing principle for a global approach to data governance. It should be noted that DFFT has been pushed by Japan in APEC, although with resistance among the developing economy members. A few APEC economies have openly expressed reservations on the use of "free" in relation to data flows.

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

under the purview of the Data Privacy Act of 2012[4] (DPA) or in other related law or policy, and if the National Privacy Commission (NPC) foresees any future implications on data localization, data sovereignty, and data protection. The BITR likewise requests for any information, views, or insights to inform and guide the BITR on the stage of the Philippines' work in terms of establishing a framework to govern cross-border e-commerce and data flows.

Free flow of data and the Data Privacy Act of 2012

Section 2 on the Declaration of Policy of the Data Privacy Act of 2012[5] (DPA) states 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. The State recognizes the vital role of information and communications technology in nation-building and 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.

The DPA indeed concerns itself with the free flow of data but limited to the specific context of personal data processing[6] only. The law has the twin task of protecting the right to privacy while ensuring the free flow of information.

This means recognizing the fundamental right of individuals to the protection of the privacy of their personal data, and at the same time, recognizing interests of the government and the private sector in the processing of personal data which is vital in the implementation of constitutional and statutory mandates and in lawful business operations, respectively.

The use of the term "free" in relation to "flow of information" is not intended to denote absoluteness in the use and/or transfer of information by personal information controllers (PICs) whether locally or across transnational borders. Any processing of personal data is still regulated and subject to the requirements of the DPA and issuances of the NPC.

We note that this interpretation is similar and consistent with other international instruments and laws on data privacy. There is a recognition that free flow of data should be facilitated but subject to the implementation of sufficient safeguards and where appropriate, conditions, limitations, or restrictions on the flow of data should be proportionate to the risks of the personal data processing activity.[7]

---

[4] 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 (2012)

[5] 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 (2012).

[6] *Id.* § 3 (j): Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

[7] See generally: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Recital 53 (4 May 2016) and Organisation for Economic Co-operation and Development (OECD) Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, Paragraphs 17-18 (Amended on 11/07/2013).

Likewise, the NPC is cognizant that cross-border data flows can have significant benefits for economic growth and that data governance is essential in the context of rapid digitalization.

The DPA does not serve as a barrier to the free flow of data across borders so long as appropriate safeguards on personal data protection are in place. This means that transfer of personal data must adhere to general privacy principles of proportionality, transparency, and legitimate purpose.[8] PICs must also ensure that recipients of personal data outside the Philippines process data in a manner consistent with requirements of the DPA and must put in place contractual or other reasonable safeguards to guarantee a comparable level of protection for data transferred.

Relevant policies on data transfers

Related to the concept of free flow of data is the principle on secure and trusted transfer of personal data. Section 21 of the DPA states that:

> Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
>
> a. The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. x x x

In the case of *In Re: FLI Operating ABC Online Lending Application*,[9] the NPC expounded that the PIC cannot surrender its accountability and responsibility to prevent any unauthorized processing under the DPA to the Personal Information Processor (PIP). The NPC ruled therein that the respondent cannot be absolved of its violations of the DPA on the argument that the processing for purposes of collections was subcontracted. The NPC explained that the respondent cannot escape the fact that it was in the position to control and exercise discretion over what personal information it processed and the extent of its processing.

In connection with the principle of accountability on transfers of personal data in Section 21 of the DPA, the NPC also issued NPC Circular No. 2020-03[10] on Data Sharing Agreements. In essence, the NPC explained that data sharing requires that the sharing, disclosure, or transfer to a third party of personal data should adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. Likewise, organizations should implement reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

Mechanisms to facilitate cross-border transfers of personal data that comply with privacy and data protection requirements and principles are likewise an area of importance. Thus, the NPC issued NPC Advisory No. 2021-02 on the Guidance for the use of the ASEAN Model

[8] Data Privacy Act of 2012, §11.
[9] National Privacy Commission, NPC 19-910 (17 December 2020).
[10] National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], (December 23, 2020).

Contract Clauses and ASEAN Data Management Framework. This Advisory recognizes the value of these initiatives to data privacy protection and trustworthy cross-border data flows and hence, promotes the adoption and use in its domestic legal framework. This Advisory also aims to provide additional guidance to supplement the ASEAN Model Contractual Clauses and ASEAN Data Management Framework as to how personal information controllers (PICs) and processors (PIPs) in the Philippines may use these in their respective personal data processing activities.

Further, the NPC continues to foster collaboration with like-minded jurisdictions in supporting privacy-respecting cross-border data flows through the APEC Cross Border Privacy Rules (CBPR) System and the Global CBPR Forum. This is in line with NPC's mission of establishing a regulatory environment that ensures accountability in the processing of personal data and promotes global standards for data privacy and protection.

Future implications on data localization, data sovereignty, and data protection

At this juncture, it would be speculative for the NPC to provide an answer to the posited question of whether the NPC foresees any future implications on data localization, data sovereignty, and data protection vis-à-vis the concept of the free flow of data.[11] Nevertheless, the NPC remains proactive in fulfilling its mandate and will respond and adapt appropriately according to the call of the times.

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 to 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

[11] National Privacy Commission, Rules of Procedure on Requests for Advisory Opinions [NPC Circular 18-01], § 5 (b) (4) (September 10, 2018).

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